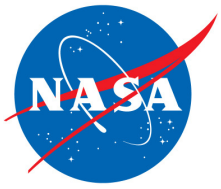
NNM09277065J



Enterprise Applications Service Technologies (EAST)

Appendix A to Attachment J-1

Cross Functional Requirements

DRAFT

16 April 2009

Change Information Page

Document History			
Document Number	Version/Change	Issue Date	Summary of change(s)
032509-2 ***041609***	***Baseline*** ***Version 2***	***March 25, 2009*** ***April 16, 2009***	***Baseline*** ***Removed requirement to submit Incident (7.3.0.j) and Problem(7.5.0ij) reports (DRDs CF-01, CF-02)***

Table of Contents

1. I3P Acquisitions

1.1 Introduction and Overview

To fulfill NASA's requirements for infrastructure improvement the Agency has directed the Office of the CIO (OCIO) to implement a program for providing more reliable and efficient Information Technology (IT) services.

As a result, NASA's OCIO established a major information technology (IT) improvement initiative in 2007, the IT Infrastructure Integration Program (I^3P). Through I^3P, the NASA OCIO intends to partner with industry to transform the way IT services are delivered and managed across the Agency.

The I³P strategy includes consolidating service demand across the Agency and working with trusted sourcing partners to deliver standardized, stable, secure, cost effective and high quality IT infrastructure and Enterprise Applications services to the NASA user community.

Specifically, the NASA I³P strategy intends to achieve the following benefits:

a. Enable Agency-wide collaboration through a seamless IT infrastructure;
b. Significantly reduce operating costs;
c. Reduce the complexity of managing IT services across the Agency; and,
d. Improve IT security across the Agency's mission environment.

In addition, the Agency intends to use this improvement initiative to enable a more process-aligned service delivery model across the scope of I^3P. This will be accomplished in part by the adoption of the IT Infrastructure Library (ITIL) framework. NASA expects selected IT Contractors to demonstrate their capabilities through the application of ITIL processes, specifically ITIL Version 3.0.

1.2 Concept of Operations

Central to NASA's I^3P initiative is the recognition that responsibility for major elements of the Agency's 'As-Is' IT environment, which is currently supported by a variety of independent Agency- and Center-based contracts, will be consolidated into a smaller number of integrated Agency-wide I^3P Contracts. Operations and service delivery must remain stable throughout phase-in periods (i.e. transition) to assure that NASA customers do not experience disruption to business operations.

NASA further expects that I^3P Contractors will work with the Agency and with each other, in a collaborative and cooperative manner as prescribed by defined processes and assigned roles and responsibilities to transform NASA's fractured IT infrastructure and enterprise applications

service delivery capabilities into a highly consolidated, integrated and secure IT Service Management (ITSM) environment.

The OCIO plans to manage this transformation through the I^3P acquisition strategy according to the following four key IT principles:

a. Mission Enabling: IT at NASA serves to achieve NASA's mission;
b. Integrated: NASA will implement IT that enables the integration of business (mission) process and information across organizational boundaries;
c. Efficient: NASA will implement IT to achieve efficiencies and ensure that IT is efficiently implemented; and,
d. Secure: NASA will implement and sustain secure IT solutions.

1.3 I³P Success Criteria

Successful implementation of the NASA I^3P vision will result in significant benefits to the Government. Specifically, NASA envisions a "To-be" state characterized by the following criteria:

a. NASA systems can be seamlessly deployed, utilized and secured across Center boundaries;
b. NASA consistently invests in the right IT solutions that provide the greatest benefit to the NASA mission;
c. NASA information is accessible, integrated, and actionable;
d. A reliable, efficient, secure and well-managed IT infrastructure is in place that customers rely on rather than compete with; and,
e. CIOs are seen as credible, trusted partners in solving business problems

1.4 Scope and Boundaries of Contracts

NASA spends approximately $1.8 billion dollars annually on Information Technology. Today, much of the infrastructure supporting NASA is decentralized including operations at NASA Headquarters, all ten NASA field Centers, and associated component locations. There are major challenges in IT management associated with a decentralized IT organization, such as lack of sufficient visibility into IT spending, inability to achieve economies of scale, inconsistent IT governance and numerous information security challenges.

NASA is consolidating IT service demand, transforming service delivery, aligning IT management and enhancing IT security through I³P. The five acquisitions making up I3P include the following enterprise services:

a. ACES (Agency Consolidated End-user Services): End-User Services – to include NASA desktops, cell phones, Personal Digital Assistants (PDAs), Agency-wide Active Directory, e-mail and calendaring functionality;

b. NICS (NASA Integrated Communications Services): Communications Services – to include data, voice, video, LAN and WAN services;
c. NEDC (NASA Enterprise Data Center): Data Center Services – to include application/data hosting and housing;
d. WEST (Web Enterprise Service Technologies): Web Services – to include public-facing website hosting and applications; and,
e. EAST (Enterprise Applications Service Technologies): Enterprise Applications Services – to include applications services associated with the NASA Enterprise Applications Competency Center and Agency-wide collaboration services including NASA's Identity, Credentialing, and Access Management (ICAM) in addition to new intranet environments and applications.

Today, these services are provided under four Agency-wide service contracts and many additional Center IT Infrastructure contracts. Some of the existing contracts are identified in the Tables below.

Location	Contract Name	Contract Number	Contractor
HQ/OCIO	NASA Web Portal Services	GS-35F-0627P	eTouch
MSFC	Unified NASA Information Technology Services (UNITeS)	NNM04AA02C	SAIC
MSFC/GRC	Compusearch Software Systems (CSS), Inc (PRISM/CMM)	NNC05QA95D	CSS, Inc.
NSSC	Outsourcing Desktop Initiative for NASA (ODIN)	NAS5-98145	Lockheed Martin Govt. Services
NSSC	Outsourcing Desktop Initiative for NASA (ODIN)	NAS5-98144	Lockheed Martin Govt. Services/OAO

Table 1: Current **Agency-wide Contracts**

Location	Contract Name	Contract Number	Contractor
ARC	Ames-Consolidated IT Services Task Order (ACITS)	NNA04AA18B	QSS Group
DFRC	Research Facilities and Engineering Support Services (RF&ESS)	NAS4-00047	Arcata Assoc.
GRC	Professional, Administrative, Computational and Engineering Support Services (PACE III)	TBD	TBD – In final stages of SEB
GSFC	Business Application and Sustaining Engineering (BASE)	NAS5-02038	Indus
HQ	Headquarters Information Technology Support Services (HITSS)	NNH06CC93B	InDyne
JSC	JSC Enabling Technology and Security (JETS)	NNJ04JA53C	MEI Technologies

JSC	JSC Information Management and Media Services (JIMMS)	NNJ04JA52C	Tessada
KSC	Information Management and Communication Support (IMCS)	NNK08OH01C	Abacus Technology
LaRC	Consolidated Information Technology Services (CONITS)	GSA GS-00T-99-ALD-0209	Raytheon
MSFC	United NASA Information Technology Services (UNITeS)	NNM04AA02C	SAIC
NSSC	NASA Shared Services Center (NSSC)	NNX05AA01C	CSC
SSC	Information Technology Services (ITS)	NNS04AB54T	CSC

Table 2: Current Center IT Infrastructure Contracts (Partial List)

The figure below represents how today's Agency-wide and Center IT infrastructure and support services contracts map into the I^{3}P acquisitions. The diagram is intended to represent the concept only and not specific contract scope decisions which are specified within the RFPs for each of the individual contracts.

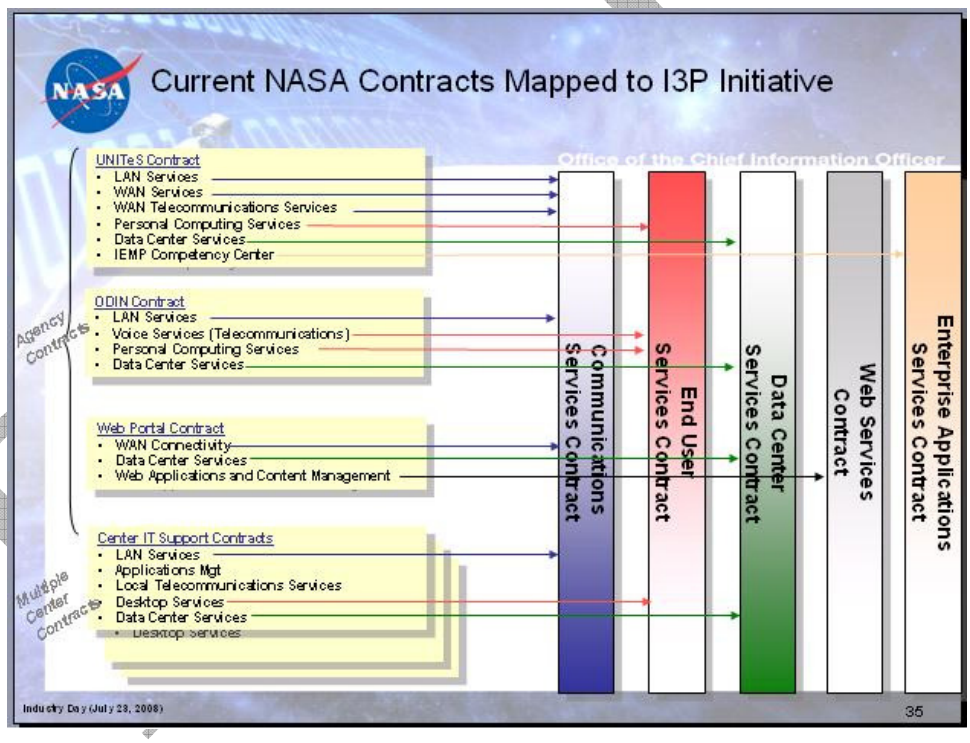


Figure 1: Concept of mapping current Agency and Center contracts to I^{3}P contracts

1.5 Client Facing and Support Services Contracts

ITIL defines client facing services as services that are delivered to end-users of the business (e.g., email, billing, etc.). Support services are defined as services necessary to support the operation of the delivered service (e.g., data center services, managed network service, etc.).

The relationship between Client Facing (Core) Services and Supporting Services is depicted in diagram below.

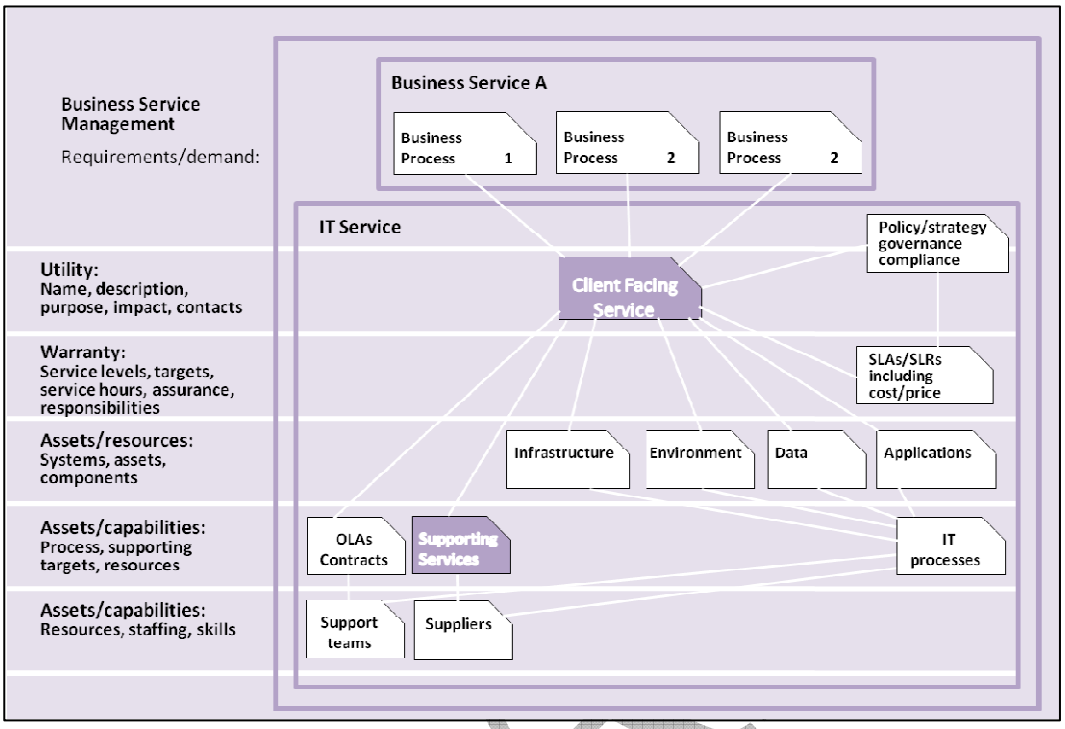


Figure 2: Relationship between client facing and supporting services

While all I^{3}P contracts will provide some level of client-facing service delivery, for the purposes of general discussion, NASA's I^{3}P contracts are classified as client facing or support service contracts as follows:

- Client Facing Contracts:
  1. ACES – End-user services
  2. EAST – Enterprise application services
  3. WEST – Web services
- Support Service Contracts:
  1. NEDC – Data center services
  2. NICS – Communication services

1.6 Cross Functional and Collaboration Activities

Each of the five acquisitions includes a Performance Work Statement (PWS) consisting of defined work activities and Contractor requirements specific to each of NASA's five

independent service contracts. These PWS's also define roles and responsibilities for the Contractor as they relate to NASA's requirements.

In addition to service-specific performance work statements, there are a number of Contractor work activities and responsibilities that cut across all five I^{3}P contracts. These Cross-Functional Performance Work Statement (CF-PWS) appendices are common to each of the procurements and define NASA's expectations for synchronization of effort and solution integration across NASA and multiple contracts supporting the I³P initiative.

Consistent application of these cross functional requirements is central to NASA's desire to standardize processes using the ITIL Version 3.0 framework and is essential to an effective, integrated enterprise service delivery.

1.7 Cascading Service Level Agreement Requirements

Service Level Agreements (SLAs) are an important aspect of NASA's service-based organization and the I^{3}P acquisitions. An SLA specifies the level, scope and quality of a service that will be provisioned, from the business customers' perspective. The SLA clarifies how the service provision will be measured, and the penalty to be exacted if the service is not delivered to the agreed level of service. To provide effective and responsive IT services across the enterprise, NASA intends to manage service levels that cascade across multiple contracts.

Service delivery under the NASA I^{3}P program will require the involvement of multiple providers to meet the SLAs established by the NASA business customer and providers are expected to work together in the best interest of NASA as described in Section 3. The diagram below depicts how an SLA will be segmented into independent Contractor service levels. Contractor-specific service levels are specified in the Service Level Matrix section of each of the five RFP's.

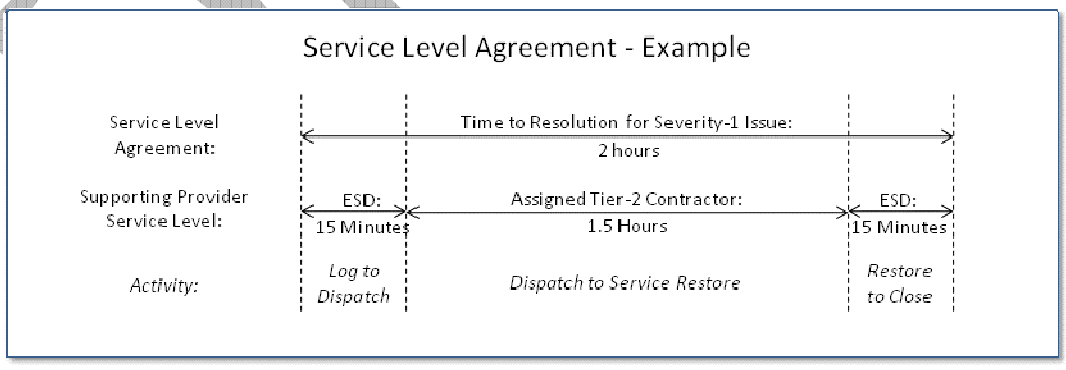


Figure 3 SLA Integration Concept

In the example diagram above, the SLA for restoration of service to the customer for a Severity 1 issue is two hours. The Enterprise Service Desk (ESD) would have a maximum time of fifteen minutes to escalate the call to the appropriate Tier 2 Contractor. At that point, as specified in the Tier-2 contractor SLA, the Tier 2 Contractor would have a maximum of one and a half (1.5)

hours to correct the problem and restore service before assigning the incident back to the ESD for call closure. After Tier 2 has reassigned the incident to the ESD, the ESD would again have a maximum of fifteen (15) minutes to verify service restoration with the customer and close the call. The sum of the ESD and Tier 2 Contractor SLAs (15 minutes + 1.5 hours + 15 minutes) would equal the customer Service Level (2 hours). In this example, only one Tier 2 Contractor is involved with the service restoration, but in some cases multiple Tier 2 providers may be involved. I^3P Enterprise Service Management leadership will coordinate service restoration efforts that span multiple providers. In all cases, Tier 2 providers are accountable only for the service level agreements specified within their individual contract. The service levels for each Contractor involved in the incident are designed to ensure that the overall NASA SLA with the end-user is achieved.

2 IT Service Management: Organization and Governance within NASA

2.1 Introduction and Overview

NASA is transforming the Agency's IT infrastructure and applications services environment through I³P. This transformation requires changes in the way NASA manages IT across the Agency including the need to define and clarify roles and responsibilities within the NASA IT organization to assure success of the I³P initiative.

As with most organizations, the NASA IT organization is continually changing and maturing to better meet the evolving needs of the customer base it serves. This section outlines the roles and responsibilities across the IT organization within NASA. Two new elements are defined to support the transformation that is underway, including the establishment of enterprise service management (ESM) functions within the Agency CIO organization and the creation of Service Integration Management (SIM) within the Agency CIO's Architecture and Infrastructure Division. Contractors providing IT services to NASA are expected to establish appropriate roles and responsibilities in support of NASA's IT Service Management (ITSM) vision as described in this section.

2.2 The NASA IT Organization: Roles and Responsibilities

The NASA CIO established the Information Technology (IT) Infrastructure Integration Program (I^3P) and is responsible for overall direction and leadership of the program, within the larger context of NASA's IT organization. Before discussing the NASA IT Organization, it is important to understand the charter and purpose of I^3P:

> **I3P Charter:** Provide a NASA Enterprise service support environment that optimizes the Information Technology Infrastructure Library (ITIL) best practice processes for implementing formal Information Technology Service Management (ITSM).
>
> **I3P Purpose:** The I³P initiative seeks to standardize NASA's IT service management practices, align with industry best practices (e.g., ITIL), and yield a set of consistent, repeatable and measurable processes for service delivery to NASA OCIO customers.

The NASA IT organization is comprised of multiple elements serving Agency, Mission, and Center customers and organizations. The elements of the NASA IT organization are defined below, including an overview of the roles and responsibilities of each part of the organization.

2.2.1 Agency CIO

The NASA CIO is accountable for all aspects of IT within NASA as well as for the overall leadership of the NASA IT organization including the establishment of strategy, enterprise architecture, and operational policies and standards to support the NASA mission. To accomplish these functions, the NASA Office of the CIO is organized into 4 divisions including Architecture and Infrastructure, Enterprise Portfolio Management, IT Security, and Policy and Investments. Within this structure the NASA CIO has also established functions associated with

Service Engineering and Integration (SE&I), Project Executives (PEs), and Service Integration Management (SIM). Through integration with the SIM, the NASA Enterprise Service Desk (ESD) provides critical integration functions in support of Agency ESM. Finally, the NASA CIO is also accountable for establishing a NASA governance model that effectively interconnects the various components of the Agency-wide IT organization and enables effective decision making at all levels within that organization. This governance spans not only the elements of the Agency CIO's office, but also Center and Mission Directorate CIO organizations; these will be described later in this document.

2.2.2 Enterprise Service Management

To support effective delivery of enterprise IT services, an Enterprise Service Management (ESM) function is performed by the Architecture and Infrastructure Division, interfacing with the other Agency CIO Divisions. ESM provides a NASA Enterprise service support environment that optimizes the Information Technology Infrastructure Library (ITIL) best practice processes for implementing formal Information Technology Service Management (ITSM). The purpose of ESM within NASA is to standardize NASA's IT service management practices, to align with industry best practices, and to yield a set of consistent, repeatable, and measureable processes for service delivery to NASA OCIO customers. Within the NASA IT structure, ESM is accountable for IT service strategy and design, integration of daily operations, overall management of enterprise suppliers, customer relationship management and continuous service improvement.

a. Service Strategy direction on how to design, develop and implement IT Service Management.
b. Service Design direction for the design and development of IT services and IT Service Management processes.
c. Service Operations direction on achieving effectiveness and efficiency in the delivery and support of IT services so as to ensure value for the customer and the IT service providers, including effective coordination across all service providers.
d. Continuous Service Improvement direction in creating and maintaining value for customers through better design, transition and operation of services.

Within the NASA Office of the CIO, ESM is responsible for overseeing service engineering and integration (SE&I), coordination of project executives (PE), implementation of service integration management (SIM), and coordination with the various I^3P project offices. Each of these ESM areas will now be further described briefly, with additional detail available in the NASA Enterprise Service Management Concept of Operations document.

2.2.3 System Engineering and Integration (SE&I)

The SE&I component of the NASA IT organization is accountable for the design of new services including the development of cost estimates associated with these new offerings. The SE&I group also ensures that new and existing services are translated into the NASA technical reference model (TRM) and that all changes to the NASA enterprise IT environment are

managed through the appropriate change advisory boards (CABs). These engineering and integration functions also include the establishment of service configuration and performance expectations, reflected in appropriate performance definitions, service metrics and evaluation criteria. Finally, under ESM, SE&I is responsible for risk assessments and impact analyses associated with the delivery of existing and new enterprise services.

2.2.4 Project Executives (PEs)

Project Executives are the actual service owners for the respective I3P services for which they have responsibility. In this role as service owners, the PEs are accountable for the configuration of services and the vetting of these services through the appropriate change control boards within the Agency. PEs are responsible for the development of their specific service strategies and the budgetary requirements to implement these strategies if approved. In order to effectively carry out their responsibilities as Project Executives, each PE must actively engage the NASA user community. This customer relationship management function is essential in identifying issues and gaps in current service delivery to support the development of strategies that will enable continuous service improvement.

Each PE also handles contract performance escalation management in those situations where an issue cannot be resolved at the project office level, or when an issue may run across multiple enterprise services and resolution requires coordination at the ESM level. In addition, managing particularly high-impact service issues that impact day-to-day performance will also be escalated to the PE for communication and possibly action. Finally, the PE is responsible for collaborating with the project office(s) responsible for the day-to-day management of service delivery to define service manager objectives and milestones.

2.2.5 Service Integration Management (SIM)

Service Integration Management (SIM) is the ESM's transformation arm responsible for process architecture and design leading to the implementation of ITIL best practices across the enterprise. Its on-going functions are to execute ESM guidance and direction. The SIM will provide support for designing and implementing the NASA Information Technology Infrastructure Library (ITIL) processes and instituting formal Information Technology Service Management (ITSM) within NASA. The Purpose of the SIM is to improve the effectiveness and efficiency of NASA IT operations through the design, implementation, and operations of standardized IT service management practices. Primary functions of the SIM include:

a. Support strategic planning associated with defining and scoping the future ITIL-aligned Service organization;
b. Direct and coordinate implementation of the strategic plan: and,
c. Provide Continuous Service Improvement and ITIL process management for NASA's IT organization

The SIM will also provide Enterprise Service Desk (ESD) oversight and integration, along with the integration of performance metrics across all enterprise services. These metrics provided by

the ESD will be used by the SIM to obtain a 'big-picture' view of service performance, leading to service improvement recommendations.. Additional information about the ESD is provided in the following section.

2.2.6 Enterprise Service Desk

The Mission of the ESD is to be the Single Point of Contact (SPOC) for Enterprise Services support, handling incidents and requests, and providing an interface for activities such as changes, problems, configuration, releases, service levels and IT Service Continuity Management. The importance of the ESD as a SPOC is to provide a single, consistent interface to the end-user community, which is a critical element of the business' determination of how well NASA IT is performing its job – one of the success criteria of the I3P program.

The primary priorities of the ESD are:

a. To manage customer expectations by identifying and communicating I3P services to customers. Route customers to the appropriate point of contract for those services not provided directly by the ESD or an I^3P service provider;
b. To return the customer to normal operations within Service Level Agreement (SLA) requirements and specifications;
c. To continually improve service performance
d. To perform consistent workflow enabling service request escalations across disparate IT infrastructure towers;
e. To provide reliable communications coordination for Enterprise Service outages;
f. To collect, consolidate, analyze, and report performance metrics across the 5 independent IT service providers for Enterprise Services provided to customers;

To provide the SIM with accurate and appropriate data that enables responsible operational decisions

To leverage existing NASA infrastructure to reduce costs; and

To provide integrated service support interfacing to functional areas of Procurement, Finance and Human Resources.

2.2.7 Project Offices

Located at each of the sites hosting an I^3P service contract, project offices are accountable for the day-to-day management and delivery of the enterprise services that they manage. Project offices are expected to coordinate across service managers, contracting officer's technical representatives (COTRs) and contracting officers (COs) to ensure the effective delivery of services across the Agency. While these offices are physically located at and managed by specific Centers, they perform an Agency function. The project offices are also responsible for the management and synthesis of I^3P contract service performance and financial information, and communication of this information through the SIM and the appropriate PE. In terms of communication, the Project Office provides information to the Agency CIO, Project Executives, Service Integration Management, and Center and Mission Directorate CIOs to ensure that all

levels of the NASA organization remain informed regarding important performance or service delivery issues. Project offices manage the day-to-day financial transactions and issues associated with the services they manage, and will escalate complex contract and performance issues as required. Project offices will work closely with the I^3P service providers to manage technical issues as well as to ensure that contractual service levels are consistently being achieved.

2.2.8 Center CIO

As with the overall NASA IT service delivery environment, the role to the Center CIO continues to evolve and mature. With the implementation of I^3P and the resulting shift from local to enterprise delivery of some services, the role of the Center CIO and the staff that they manage is evolving. Even as the roles and responsibilities shift to support the NASA IT strategy, the Center CIOs maintain significant responsibility for local service delivery, and are acquiring new roles associated with enterprise service strategy and delivery. These roles and responsibilities are described in the following section.

Relative to local service delivery, Center CIOs are accountable for the day-to-day delivery of locally-provided IT services that are not provisioned as part of one of the Agency service contracts. This includes all aspects of managing these services including service design, implementation, monitoring, security, and continuous improvement. The Center CIO is also accountable for ensuring that any locally-provided services align with Agency strategy and policy. Center CIOs ensure the provisioning of local infrastructure to enable effective and efficient delivery of enterprise services while overseeing the Center's overall IT portfolio and managing demand for both local and enterprise services. The CIO is ultimately responsible for customer relationship management across all organizations at the Center, and ensures that requirements, issues, and concerns regarding IT services are captured, understood, and addressed. In terms of strategic leadership, each CIO is a member of the Center's executive leadership team responsible for solving business problems through the application of innovative IT solutions. In a similar manner, each Center CIO is a member of the Agency IT Management Board and is responsible for setting the Agency's strategic direction relative to information and information technology.

Center CIOs also have significant responsibility relative to enterprise service delivery. Because the Agency has such a highly-skilled IT workforce spread across all Centers, each CIO will identify subject matter experts (SMEs) to support each of the enterprise services at their respective Center. In addition to these SMEs, a Center Integration Lead will be identified to coordinate and manage issues involving integration across multiple services. These SMEs and Integration Leads will work closely with the associated Project Offices and the Agency SIM to effectively implement enterprise delivery of key services. As additional requirements are identified for new or improved services, Centers CIOs will also identify and provide technical experts to participate on Agency-level technical and architectural teams. Finally, the CIO will serve as the voice of the Center customers to Agency service providers while monitoring service integration and performance issues locally and participating in continuous service improvement efforts.

Those CIOs whose Centers host Project Offices have additional responsibilities including working with the Agency CIO to determine the appropriate staffing levels for the office and then staffing the office as agreed. Host Center CIOs also work with the appropriate PE(s) to define performance objectives for local staff members who are supporting enterprise service delivery and then manage the project office staff to ensure that the Center delivers on these Agency commitments.

2.2.9 Mission Directorate CIOs

Similar to Center CIOs, Mission Directorate CIOs represent the requirements of their respective missions, which cut across all NASA Centers. The Mission Directorate CIO has a unique understanding of the mission requirements related to information and information technology and works with Center and Agency IT Service providers to ensure that these requirements are satisfied. Each Mission Directorate CIO is a member of the Agency IT Management Board and is responsible for helping to set the Agency's IT strategic direction and provides a critical customer relationship management function, service as the voice of the mission customer regarding all aspects of NASA IT services.

2.3 NASA IT Governance Process and Structure

Contractors are expected to adhere to the NASA OCIO governance strategy and framework as outlined in this section and discussed in greater detail within each respective I³P acquisition Request for Proposal and associated performance work statements.

By conforming to NASA's IT governance process, Contractors will assist the Agency in its efforts to:

- Support the NASA Mission via ongoing alignment and management of NASA's IT assets and processes with its mission requirements and strategic initiatives;
- Identify potential areas of investment redundancy and opportunities for consolidation, rationalization and cost efficiency; and,
- Conduct master planning at the Agency level to increase visibility of and better prioritize investments.

NASA's approach to IT governance is a structured, decision-oriented model that has critical linkages to NPR 7120.7 NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements and other NASA IT management processes such as capital planning and investment, information technology security planning, and enterprise architecture as defined in various IT-related policy documents (NPR 2800.1, Managing Information Technology, NPR 2810.1 Security of Information Technology, and NPR 2830.1 NASA Enterprise Architecture Procedures).

NASA's IT environment is organized into three major areas, or portfolios:

- IT infrastructure services;
- IT applications; and
- Highly-specialized IT, such as technology that supports real time control systems and on-board avionics.

While some cross-cutting IT processes, such as IT security, apply to all portfolios, the scope of IT governance described in this section applies primarily to IT infrastructure and application services.

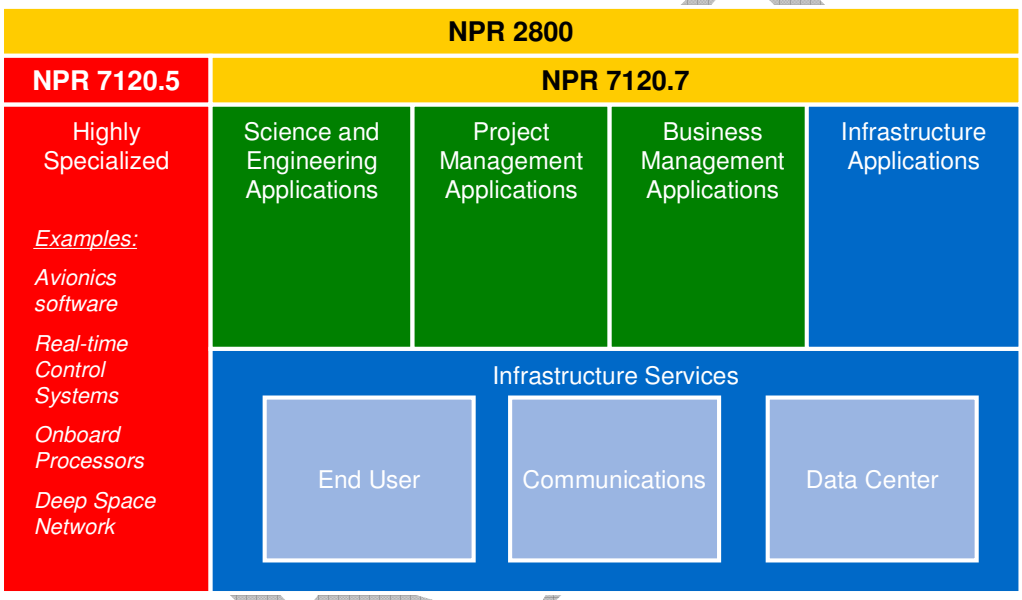


Figure 4: IT Portfolios and Governing Policies

To address the wide-ranging decisions which are likely to occur throughout the life cycle of the I³P contracts, at an Agency level NASA will employ a three-tiered board model where each board has a clear set of responsibilities as well as interfaces to the other governing bodies. This governance model shown below provides complete coverage of the life cycle of an IT investment from the initial decision to fund a proposed investment to the oversight of its implementation and operations and subsequent decommissioning. Each of these life cycle phases has associated with it unique milestones and metrics that require different activities and therefore different board oversight.

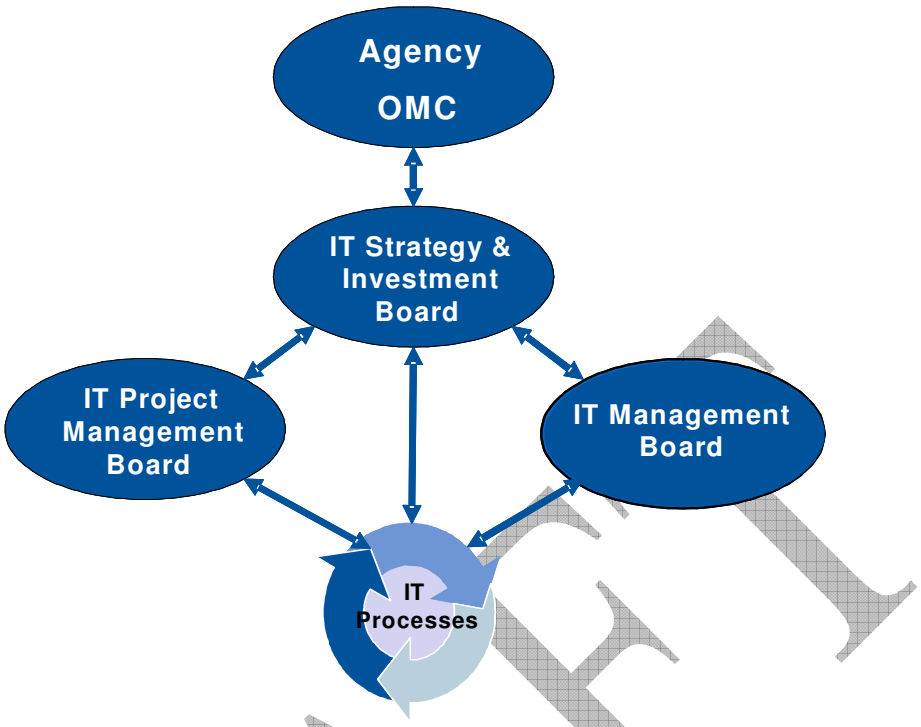


Figure 5: NASA IT Governance Structure

The scope and purview of each NASA board is further defined as follows:

- **IT Strategy and Investment Board (SIB)** – Decisions regarding IT strategy and related investments (prioritization and selection), Enterprise Architecture, and NASA-wide IT policies/processes. Members include senior level stakeholders from Mission Directorates, Mission Support Offices, and Centers.
- **IT Project Management Board (PMB)** – Decisions regarding application and infrastructure projects to ensure that investments approved by the IT Strategy and Investment board stay on track during formulation, design and implementation. Members include the Deputy CIO, one or more IT Strategy and Investment Board representatives, IT Operations Board Chair, Enterprise Architecture (EA) Lead, and representatives from Mission Directorates, Mission Support and Centers.
- **IT Management Board (ITMB)** – Decisions regarding operational performance and issues related to performance. Members include the Associate CIO for Architecture and Infrastructure, Center CIOs, the Deputy CIO for IT Security and the EA Lead. Mission Directorates may provide a representative at their discretion.

Although each governance board is chaired by a member of the OCIO, decisions are made in consultation with and in concurrence with key stakeholders. Should the need arise an escalation path exists to the Agency Operations Management Council (OMC) which can be invoked as necessary.

The governance structure described above operates at the Agency level and addresses major IT investments that cross Center and program boundaries. Centers are also implementing local governance structures that while customized to the unique organizational environment and culture at each Center, conform in spirit to the Agency governance structure and enable Center-specific investments to be addressed. Notwithstanding the existence of Agency or Center specific governance structures, it is expected that changes will need to be made over the life of the I³P Acquisition to address the full IT life cycle as described in NPR 7120.7.

NASA's approach to IT governance reflects the latest in industry best practices and is grounded in the strategic management principles for governing, managing, implementing, monitoring, and controlling the work of the Agency as set forth in the Strategic Management and Governance Handbook NPD 1000.0.

2.4 Contractor Responsibilities

In addition to working with NASA in concert with Agency level governance processes and structures, Contractors must work within other complementary contract and relationship management mechanisms as defined within each tower specific Request for Proposal (RFP).

These additional governance processes and structures relate to the Contract administration and management activities that are specific to the individual NASA Centers responsible for procuring and overseeing delivery and performance as defined in the individual I³P performance work statements. Contractors should refer to the individual RFPs for details of these complementary governance processes and structures.

NASA expects I^{3}P Contractors to work closely with the ESM and SIM organizations to ensure adherence to NASA standard IT processes, monitor compliance, drive continuous service improvement and coordinate service operations to achieve an effective and efficient multi-sourced IT environment in support of Agency requirements.

While specific requirements are captured in the cross-functional ITIL process requirements, an overview of these responsibilities associated with supporting ESM and SIM activities is provided below.

Policies and Procedures: Contractors are responsible for supporting SIM identify, define and implement changes to Agency IT policies and procedures that improve service delivery, streamline operations and reduce costs. Contractors are expected to do this through the identification and application of Industry best practices, methodologies and tools within the NASA ITSM environment.

Strategy Development: Contractors will participate in the Agency's annual portfolio management process by providing design, cost, benefit, risk and other information necessary for the SIM to prioritize as recommended list of projects aligned with user requirements.

Process Development: Contractors will support service integration by defining and implementing service delivery processes and procedures identified in the Agency's Cross Functional Statement of Work and other Contractor processes that are complementary to NASA's ITIL v3 aligned processes.

Process Interface: Contractors are responsible for ensuring that cross-tower service integration and delivery touch-points are aligned with both Government and other I³P Contractors so that seamless service delivery and management occurs.

Compliance Monitoring: Contractors are responsible for supporting the Agency in monitoring of service delivery to the end customer. Such monitoring will include but not necessarily be limited to process quality assurance, escalating and resolving issues (inclusive of cross-tower/vendor), monitoring production control, and integrating actions, communications and exchanges of service supporting data activities across I³P Contractors to ensure customer support requirements are met (i.e. SLAs are met).

Operations Coordination: Contractors are responsible for supporting NASA's management of the multi-sourcing environment by supporting coordination and oversight of operations.

Continuous Improvement: Contractors are responsible for identifying, defining and implementing continuous service improvement activities. Contractors are also responsible for benchmarking projects as defined by SIM's continuous improvement processes.

2.5 Relationship Management

Contractors are expected to follow a robust Governance model to partner with NASA and manage both services delivery and contract performance. Relationship management focuses on actively managing relationships with NASA customers, stakeholders and other Contractors who are integral to the delivery of integrated IT service management (ITSM) under I³P. All relationship management practices are ongoing and entail the following set of activities:

- Managing interactions with NASA to ensure their effectiveness and to capture critical service level information;
- Formally managing relationships with NASA customers and Contractors by establishing relationship objectives and tracking performance of those objectives;
- Selecting suppliers and partners based on their ability to meet NASA business requirements and managing their performance on NASA's behalf;
- Obtaining feedback from NASA stakeholders, including employees, and Contractors on the nature and quality of key service and delivery relationships; and,
- Proactively identifying opportunities that will provide additional value to NASA.

The NASA IT governance structure is designed to encourage collaborative discussion of issues and ideas critical to the ongoing success of I³P and related IT transformation. As detailed in the individual I³P acquisitions, each party will designate an individual to serve as a relationship manager who will be that party's single point of contact (SPOC) for all matters relating to the outsourcing contract. The contractor's relationship manager:

- Must be knowledgeable about NASA's I³P service requirements and each of the contractor's and its sub-contractors / partners products and services;
- Must be experienced at running IT systems and networks, as they relate to the provision of services for which they are contracted, of similar size to NASA's current and anticipated business requirements;
- Must have overall responsibility for directing all of the Contractor's activities; and,
- Will be assigned to the NASA account for a significant portion of the contract term.

NASA expects that Contractors will assist and contribute to setting the strategy and policy concerning NASA's technology and use over the life of each I³P contract. Contractors should be continually evaluating the technical environment, identifying potential enhancements that will reduce overall costs while delivering high quality and high availability services across the Agency.

3 Service Coordination and Collaboration

3.1 Introduction and Overview

The I³P Acquisitions involve more than management of five independent sourcing agreements. The effort will require coordination, collaboration and integrated management of key processes across Contractors and contract boundaries.

It is in the coordination of multiple Contractors where the management of I3P services differs from the management of five independent IT contracts. Coordination of services across these multiple contracts involves coordinated management of four sets of relationships:

a. Between NASA end users and individual Contractors;
b. Between NASA leadership and individual Contractors;
c. Between NASA's internal client facing and support organizations required to deliver IT services; and,
d. Between the I^3P Contractors.

It is important that Contractors work with NASA and with each other to establish and execute common management approaches and procedures to ensure that services are provided effectively and efficiently across the enterprise regardless of contractual boundaries.

3.2 Service Coordination, Collaboration

NASA recognizes the interdependencies of internal and external relationships and expects contractors to work with the Agency and amongst themselves, to manage those interdependencies proactively.

Contractors are expected to ensure that processes and procedures are established and maintained to support service coordination and collaboration with NASA and other I^3P Contractors in the following delivery areas.

a. **Service Delivery Strategy** – Proactive management of NASA's service delivery strategy assumes that business conditions and customer requirements change over time requiring that initial strategies adapt to changes as they occur. By working with NASA to modify goals, priorities, policies and procedures as they affect one or more of the sourcing relationships, I^3P Contractors are expected to continuously improve how services are delivered to meet end user needs.

b. **Service Delivery Responsibility** – Management of service delivery can be complex when multiple Contractors are responsible for IT service delivery. I^3P Contractors are expected to know and understand who is responsible for each service delivery task, where touch-points or hand-offs are and how their responsibilities change as end-to-end service

delivery crosses contract boundaries. Process flows, cross-functional and contract-specific performance work statement elements all play a part in defining roles and responsibilities where coordination is required to ensure continuity of service and operations.

c. **Service Delivery Integration** – Coordination and collaboration across multiple Contractors demands that multiple Contractors work together and as needed, co-develop processes that define the rules of engagement between various parties as well as how to manage the many touch-points and interface requirements between Contractors, end-users, and internal NASA organizational entities. Proactive management of delivery integration not only ensures that everything that needs to get done is accomplished, but that Contractors work together to identify, create and document any new procedures necessary to ensure seamless service delivery to NASA customers over time.

d. **Service Delivery Value and Funding** – Proactive management of this process is focused on ensuring that end-users receive the expected value for services delivered and that business goals are being met over time. Furthermore, Contractor coordination and collaboration in this area is intended to ensure that Contractors are fairly compensated for the services they deliver and no one Contractor is disadvantaged because of lack of clarity around responsibilities, touch-points or integration interface requirements.

e. **Service Delivery Performance Assessment** – Proactive management of service performance processes are focused on verifying the facts of the relationship through coordination and cooperation among NASA I^3P and supporting Contractors. Cooperation is expected to occur in support of service level evaluations, operational or security assessments, financial audits, and other assessments required by the OCIO in response to changing business conditions or governance requirements.

f. **Delivery Communication** – Proactive management of communications and feedback requires the transmission of information generated throughout service creation and service delivery processes. Reporting processes need to adequately address end-to-end service delivery requirements, ensure the right information is available to the right people at the right time, and facilitate operational excellence and support NASA's decision making requirements.

NASA's Enterprise Service Management organization will be the focal point to ensure seamless IT service delivery.

4 NASA IT Infrastructure Library (ITIL) Version 3 Approach

4.1 Introduction and Overview

In support of the Agency Chief Information Officer's (CIO) vision for I^{3}P, various IT operational models were analyzed and the Information Technology Infrastructure Library (ITIL) version 3.0 framework was selected. Applicable ITIL v3 processes have been identified and prioritized for development and implementation within the NASA IT environment. It is recognized by the NASA Information Technology Management Board (ITMB) that a common and consistent Agency-wide IT organizational management structure is required to support centralized, Agency-provided IT services. The new ITIL processes will be designed to enable and support IT governance via performance metrics. The adoption of a standardized framework that includes a common terminology and process set will be an integral part of all I3P support contracts. ITIL version 3.0 focuses on Service Management and seeks to align IT with business objectives. ITIL version 3.0 outlines a set of integrated processes that encompass the full scope of the IT service lifecycle. By defining a common set of ITIL version 3.0 aligned processes that are applied across all I^{3}P contracts, NASA strives to attain maximum efficiencies while ensuring seamless, integrated services for IT customers.

Adoption of ITIL will enable NASA's mission by:

a. Better integrating the agency's people, processes, and information;

b. Improving security; and,

c. Achieving cost savings.

4.2 Implementation Plan and Scope for I^{3}P

NASA has developed an implementation plan and roadmap based on the introduction of ITIL v3 as the Agency's process framework in support of I^{3}P. Prospective service providers shall have documented, repeatable ITIL processes with relevant metrics reporting capabilities. NASA requires prospective service providers to engage and align with NASA's IT organization and NASA's ITIL processes.

NASA's approach is based on a phased implementation of ITIL processes. Activities in support of this implementation have been prioritized according to the following Government criteria:

a. Processes having greater relative importance to I^{3}P Acquisition Governance and Strategy;

b. Processes that require extensive, multiple vendor coordination and integration; and,

c. Processes that industry experience and best practice suggest should be addressed earlier in an ITIL implementation

Twelve (12) of the ITIL v3 processes have been grouped into either Primary or Secondary implementation priorities.

Five (5) of these processes have been identified as primary implementation priorities. They include:

a. Change Management;
b. Incident Management;
c. Request Fulfillment;
d. Problem Management; and,
e. Service Level Management.

These five processes are considered primary I3P implementation priorities for the following reasons:

a. They are foundational processes in that many of the remaining ITIL processes depend on them;
b. They have strong ties to the new Enterprise Service Desk (ESD) being established in support of the I3P acquisition and cross all five (5) of the independent service contracts;
c. They tend to be ticket-management-heavy processes central to efficient and effective resolution of service interruptions and/or restoration of services to end-users;
d. There is stronger familiarity of these processes among the NASA technology groups; and,
e. There are significant opportunities associated with these processes for quick wins and/or accelerated achievement of I3P objectives.

Seven (7) of the ITIL processes have been identified by NASA as secondary I^3P implementation priorities. They include:

a. Service Asset and Configuration Management;
b. Release and Deployment Management;
c. Capacity Management;
d. Strategy Generation;
e. Service Portfolio Management;
f. Service Catalog Management; and,
g. Supplier Management

These seven processes were targeted as secondary implementation priorities because:

a. Several (e.g. Release and Deployment Management and Capacity Management) require that Change Management be in place and operational prior to their implementation;
b. Several (Service Asset & Configuration Management and Service Catalog Management) require significant set-up and coordination across the I3P contracts and delivery teams; and,
c. Several (Service Portfolio Management, Supplier Management and Strategy Generation) are critical to establishing strategic direction for I3P and create momentum behind its execution.

The remaining fifteen (15) ITIL v3 processes are considered tertiary implementation priorities by NASA. Selection and prioritization of these for implementation will be evaluated and determined as the NASA ITIL framework matures. They include:

a. Demand Management;
b. IT Financial Management;
c. Information Security Management;
d. Availability Management;
e. Service Continuity Management;
f. Validation and Testing;
g. Transition Planning and Support;
h. Knowledge Management;
i. Event Management;
j. Access Management;
k. Operations Management;
l. Service Evaluation;
m. Service Improvement;
n. Service Reporting; and,
o. Service Measurement.

In summary, NASA's introduction of ITIL v3 processes in support of the Agency's I3P Acquisition supports the Agency's goals of transforming NASA's current environment to a more highly integrated IT Service Management environment.

4.3 NASA Defined ITIL v3 Process Requirements

I^{3}P Contractors shall define and implement service delivery processes and procedures that are consistent with both individual service provider-specific and cross-functional performance work statement elements.

I^{3}P Contractors shall implement processes and procedures that are consistent and complementary to NASA ITIL v3 aligned processes.

I^{3}P Contractor interfaces associated with NASA IT services shall support NASA's ITIL process requirements as detailed in the cross-functional PWS elements, as well as any standards as identified in the Government process and policy documents associated with each NASA IT process.

Contractors shall actively participate in supporting changes to NASA process and policy documents. Changes to NASA process and policy documents will be managed by the Office of the Chief Information Officer.

5 I^{3}P Common Architecture Components

5.1 Introduction and Overview

NASA's strategic approach to the management of IT infrastructure is to provide Enterprise-wide infrastructure services to maximize efficiency, improve IT security, and provide the best possible user experience. These infrastructure services have been defined into 5 different portfolios:

a. End-User Services
b. Network and Communications Services
c. Enterprise Data Center Services
d. Enterprise Applications, and
e. Web Services

Each of these portfolios provides a specific set of component services which comprise part of the NASA Enterprise Architecture as reflected in the NASA Enterprise Service Catalog. Common across these 5 portfolio areas is the requirement for a TIER-0/1 Enterprise Service Desk (ESD) and an Enterprise Service Request System (ESRS). Finally, to reduce redundancy and promote interoperability and collaboration, applications within the NASA environment must be integrated through the NASA Application Portfolio Management process. Each of these elements of the NASA environment is further described below.

5.2 NASA Enterprise Architecture Repository

In support of the continual evolution of the NASA Enterprise Architecture (EA), a knowledge base known as the NASA Enterprise Architecture Repository (NEAR) is being developed to support all Agency enterprise architecture and related activities. The development of NEAR has resulted in the creation of an EA repository data model and ontology to allow mapping, integrating, rationalizing, and normalizing existing repositories and data stores into the NASA EA Framework. The effort also involves the development of integration strategies for structured, semi-structured and unstructured data, the analysis of functionality supported by existing data sources for possible consolidation into the EA repository, and the creation of web-based access methods to streamline NEAR population, maintenance, and analysis.

The NEAR will support the Alignment of IT goals, services, systems, components and standards with Center, Mission Directorate, and Agency goals, while enabling more effective management of current assets and improved planning for new investments. In addition the NEAR will reduce information redundancy and improve data consistency while at the same time increasing flexibility and agility to provide a vision of the future state of the IT environment and to reduce costs. Data requirements associated with the NEAR are documented in the NASA Enterprise Architecture Repository (NEAR) Interface Definition Specification.

5.3 NASA Enterprise Service Desk

The ESD is a foundational component of NASA's I^3P strategy for delivery of core IT infrastructure services. The ESD will serve as the single point of contact for Enterprise Services support and provide a unified interface between the customer and NASA IT Service Providers. The ESD will provide TIER 0 and TIER 1 support for a multi-tenancy set of services being provided to NASA by a number of I^3P support contracts. All incidents will route through the ESD. In addition the ESD will not only handle incidents, problems and questions, but will also provide support for other activities such as customer change request processing, SLA metrics collection and reporting, services configuration management support and IT service continuity management. In addition to providing Tier-1 services, a TIER 0 (Self-Service) Service Desk Web site will be provided. This Website will provide user self-service when an incident is encountered. Information such as current I^3P infrastructure services status, I^3P services Frequently Asked Questions (FAQs), ESD Knowledge Database references, and Wiki threads will be established, monitored and updated.

The ESD will be managed by NASA Shared Services Center (NSSC) with the NSSC's Service Provider providing technical support services under the management of the NSSC. TIER 2 and TIER 3 service desk support services shall be provided by the I^3P contractors supporting the I^3P ACES, NICS, NEDC, EAST and WEST contracts. The ESD will support continuous service improvement across all I^3P services through the collection and analysis of performance metrics. The ESD will provide consistent, reliable communications and coordination of Enterprise Service outages while assisting the I^3P Enterprise Service Management organization with consolidated reporting, trend analysis, and integration support across all services.

The Enterprise Service Desk will utilize the ITIL framework and associated processes common to all I^3P service providers as outlined in the cross-functional PWS elements defined in this document. ITIL processes are divided between Service Delivery and Service Support with the Enterprise Service Desk being the primary point of contact between IT and users of IT services. The Enterprise Service Management organization in the OCIO Architecture and Infrastructure Division is responsible for the definition and development of all NASA ITIL processes. Service Support provides for implementation of operational processes and day-to-day management of the environment. Service Delivery is associated with the tactical processes and planning processes.

Additional information concerning the ESD can be found in the Enterprise Service Desk Concept of Operations, and the Enterprise Service Desk Performance Work Statement reference documents.

5.4 NASA Enterprise Service Request System

To ensure a seamless user experience, another element of the I^3P common architecture is the NASA Enterprise Service Request System (ESRS). The ESRS is envisioned to include:

a. A user-friendly, customer-facing interface to order all I^3P-provided services

b. The ability to provide pricing for services offered

c. Workflows to enable purchase authorization and verification of available funding

d. Workflows to enable the efficient distribution of component orders to the appropriate I3P service provider(s)

e. An interface to the NASA Enterprise Service Catalog to facilitate service ordering

f. The ability to track the status of all orders

g. Reporting capability to enable NASA leadership to monitor SLA performance and continuously improve service delivery

h. Integration with the Enterprise Service Desk to facilitate the aggregation of critical performance parameters with other I^3P metrics

The ESRS will be based upon the same platform as the Enterprise Service Desk and will support the ITIL service request processes detailed in the cross-functional section of this PWS. An ESRS interface requirements definition document will be provided after contract award to all I^3P service providers to facilitate the integration of provider systems with the ESRS.

The ESRS is anticipated to be operational and fully-functional to support the phase-in of all I^3P contracts. Contractors should plan for a period of integration and testing to integrate any contractor order fulfillment systems with the ESRS.

5.5 NASA Application Portfolio Management

Another critical component of the NASA environment is the NASA application portfolio. Within NASA, Application Portfolio Management provides a framework that facilitates decision making regarding application investment, development, maintenance, and decommissioning. In order to assist in effectively managing the NASA application landscape, Section 7 of this document includes process requirements associated with NASA Application Portfolio Management.

6 Common Information Technology Security Requirements

6.1 Introduction and Overview

In order to appropriately secure NASA systems and information, the following IT security requirements apply to all I^{3}P service providers. Where the term "information system" is used this refers to any system that physically or logically is connected to a NASA network, or that stores, processes, or transmits NASA data. Where NASA, federal, or IT Security policies or procedures are referenced, these may be downloaded from the NASA IT Security documentation website at http://itsecurity.nasa.gov/policies/index.html. Additional IT Security requirements may be contained in the service-specific PWS of each I^{3}P RFP and must be followed in addition to the requirements contained in this cross-functional section.

6.2 Common IT Security Requirements

a. All information systems provided and/or operated under this contract are federal information systems. (A federal information system is defined in NIST SP 800-37, Rev 1, *Guide for the Security Authorization of Federal Information Systems* and in 40 U.S.C., Sec. 11331, as an information system used or operated by a federal agency, or by a contractor of a federal agency or by another organization on behalf of a federal agency.) The contractor shall be responsible for meeting the requirements for security authorization, also known as certification and accreditation (C&A), of these information systems, consistent with FIPS 200 and NIST SP 800-37 (Rev 1). A NASA official, determined in accordance with NPR 2810.1, shall perform the role of the authorizing official for all such information systems.
   1. The contractor shall use NASA processes, as specified in NASA policy and procedures, to meet the requirements for security authorization of all such information systems.
   2. For all information systems provided under this contract NASA will determine the system's FIPS 199 security categorization. For any other information systems provided under this contract or used in performing this contract, NASA will approve the system's FIPS 199 security category.
   3. The contractor shall ensure that all systems institute information security controls in accordance with NIST SP 800-53.
   4. The contractor shall support all applicable security assessments of each information system. At the discretion of the NASA authorizing official, the contractor shall either perform or provide for the performance of system security assessments, or support independent system security assessments (e.g., third party certification, IG Audits, GAO audits, and self certification), as part of the security authorization and continuous monitoring process.
   5. The contractor shall track identified risks and security vulnerabilities for each information system in the NASA C&A Documentation Repository and remediate vulnerabilities on a schedule as determined by the NASA authorizing official.
   6. All required system security documentation shall be entered into the NASA C&A Documentation Repository.

b. The contractor shall identify an IT Security POC for supporting IT security requirements under this contract.
c. The contractor shall configure and maintain operating system and software on all information systems provided under this contract in accordance with Federal and NASA security configuration policies and guidance.
    1. The contractor shall apply all relevant Federal system and software security configurations, for example, the Federal Desktop Core Configuration, according to NASA guidance.
    2. All information systems shall be patched with all critical patches (as determined by the product vendor or NASA) in accordance with the NASA Organization Defined Values for NIST SP 800-53 Security Controls and subsequent revisions.
    3. In some rare circumstances, the NASA Deputy CIO for IT Security or designee may determine that a particular patch must be applied more urgently. In such cases, all information systems shall be patched in the timeframe specified by the NASA Deputy CIO for ITS or designee.
    4. System configurations and patching status for all information systems provided under and in support of this contract shall be reported using the NASA patch reporting environment. Each computer shall either run up-to-date reporting agent software for automated reporting or be reported manually by the contractor. For any computers that cannot run the reporting agent software, a NASA-approved waiver must be obtained in accordance with NASA policy and procedures.
d. All information systems shall be protected by the NASA enterprise anti-malware (including anti-virus, anti-spyware, etc.) solution, which provides automated updates of virus definitions at least once every 24 hours and automated logging and reporting. The NASA enterprise anti-malware solution for desktops and laptops is provided by the ACES contract. The NASA enterprise anti-malware solution for servers is provided by the NEDC contract. For any computer that cannot use the anti-malware solution or for which no anti-malware software exists, a NASA-approved waiver must be obtained in accordance with NASA policy and procedures.
    1. The contractor shall correct or mitigate detected vulnerabilities in accordance with NASA policy, unless directed otherwise by NASA for specific urgent issues.
e. All information systems provided under this contract or used in support of this contract shall be scanned for vulnerabilities in accordance with NASA policy.
    1. The contractor shall make available all information systems located within the NASA network perimeter for network-based vulnerability scanning by NASA. NASA will coordinate scanning activities with the contractor to the extent possible to ensure that vulnerability scanning creates minimal impact on operations.
    2. For all other information systems which process NASA data, the contractor shall report to NASA the results of vulnerability scans and remediation, in accordance with NASA guidance.
f. The contractor shall follow NASA IT security incident management procedures in accordance with NASA policies and ensure coordination of its incident response team with the NASA Security Operations Center (SOC). The contractor shall report to the NASA SOC any suspected computer or network security incidents occurring on any systems, in accordance with Federal mandates and NASA policies and procedures.

The contractor shall provide all necessary assistance and access to the affected systems so that a detailed investigation can be conducted, problems remedied, and lessons learned documented. Security logs and audit information shall be handled according to evidence preservation procedures.

1. The contractor shall make available logs from any information system to the NASA common logging environment, as requested by the NASA SOC. Electronic raw log data shall be forwarded from the source device to the NASA common logging environment, in accordance with NASA policies, procedures and guidance.
2. The contractor shall provide the NASA SOC real-time, electronic access to all asset information and configuration management information for all devices provided under this contract and in support of this contract.
3. The contractor shall report the theft or loss of any device that may contain NASA information, in accordance with NASA incident reporting policy and procedures.

g. The contractor shall provide a logging environment that centrally captures and retains logs from all information systems provided under this contract.
h. The contractor shall ensure that all individuals who perform tasks as a system administrator, or have authority to perform tasks normally performed by a system administrator, possess knowledge appropriate to those tasks, as demonstrated by holding industry-standard certifications. In addition, system administrators shall not be granted elevated privileges to information systems covered under this contract unless they are authorized and have met the training requirements in accordance with NASA policy.
i. Prior to deployment of any IT security services, the contractor shall obtain approval from the NASA Deputy CIO for IT Security or designee. Any IT security services provided by the contractor shall be coordinated and integrated with the NASA SOC.
j. The contractor shall support the integration of NASA SOC IT security services and technologies into systems provided under this contract and in support of this contract, in accordance with NASA guidance.
k. The contractor shall work with the NASA OCIO and the incumbent contractor to transfer responsibility for all IT security requirements for existing information systems within the scope of the contract from the incumbent contractor to the successor contractor. The contractor will receive from NASA a list of the applicable information systems.

7 Cross Functional Performance Work Statement Elements

The NASA IT Infrastructure Integration Program (I^3P) requires coordination, collaboration, and ultimately co-management of key processes across I^3P Service Contractors and contract boundaries. To ensure a successful integrated IT service environment across NASA, it is essential that IT service providers adhere to the NASA ITIL framework. The purpose of the following Cross Functional Performance Work Statement Elements (CF-PWS) are to consolidate the requirements that must remain consistent across Contractor service agreements. The requirements contained in this section are the responsibilities of the Contractor or Contractors associated with the Cross Functional Services. NASA process documents referenced in this section can be found in the Technical Library on the I^3P web site located at http://i3p.nasa.gov/ .

7.1 General Provisions

7.1.1 IT Infrastructure Library® Version 3 (ITIL® v3) Support

Contractor shall be responsible for:

a. Defining and implementing service delivery processes and procedures that are consistent with the requirements contained in this CF-PWS. Contractor processes used to provide services shall be consistent and complimentary with Government ITIL® v3 aligned processes.
b. Ensuring that interfaces with Government, I^3P Contractors and other Contractors are consistent with Government ITIL® v3 aligned processes.
c. Ensuring that changes are approved and authorized by Government in accordance with Government Change Management Process.
d. Providing information to support maintenance of Government Enterprise Service Catalog.

7.1.2 Understanding and Knowledge of ITIL®

Contractor shall be responsible for:

a. Ensuring that all Contractor personnel involved in delivery of services shall possess, at a minimum, ITIL® foundation or equivalent ITIL® training within 6 months of contract start.
b. Providing verification that Contractor personnel, required in delivery of services, are experienced and trained in ITIL®.
c. Participating in an objective assessment of Contractor ITIL® maturity.

7.2 Change Management

7.2.0 High-Level Process Flow Diagram, Goal, Purpose and General

Goal: The goals of Change Management are to: Respond to the customer's changing business requirements while maximizing value and reducing incidents, disruption and re-work; and respond to business and IT requests for change that will align services to business needs.

Purpose: The purpose of Change Management is to ensure that: Standardized methods and procedures are used for efficient and prompt handling of Changes; Changes to service assets and configuration items are recorded in the Change Management Data Base (CMDB); and overall business risk is optimized.

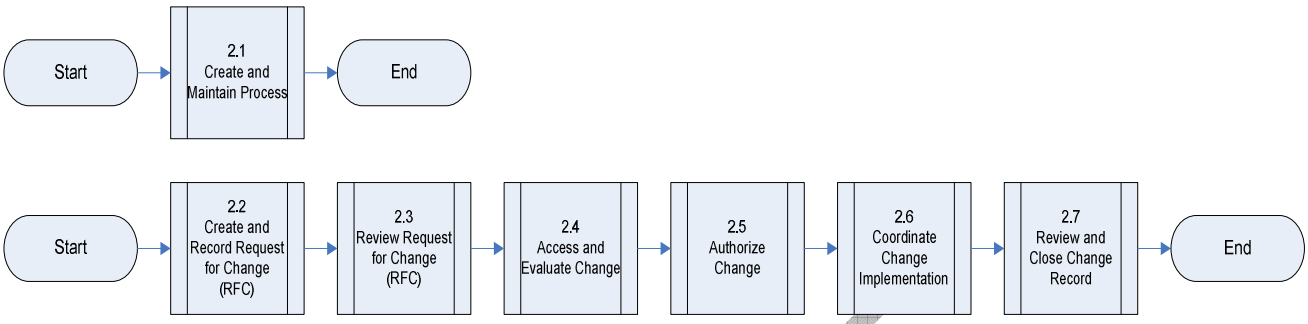


Figure 6: High-Level Change Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for:

a. Designing and implementing Change Management procedures that align with Government Change Management Process**.**
b. Documenting, tracking and managing all Changes using a Contractor or Government provided Change Management system.
c. (When Contractors use a Contractor Change Management System) Providing integration between Contractor and Government Change Management systems including the integration of applicable software, e-mail and telephony in accordance with Government Change Management Process. All changes necessary to provide system integration shall be made at Contractor expense. Contractor solution shall provide an efficient transfer of information between systems in accordance with DRD 1293CF-011, *Interface Definition Agreement (IDA)*.
d. Providing communications to users via Enterprise Service Desk and maintaining regular communications between all parties through resolution in accordance with Government Change Management Process.
e. Providing case ownership of Change Requests that are assigned to Contractor until Change record is closed or ownership is reassigned.
f. Participating in regularly scheduled Change Management meetings in accordance with Government Change Management Process.

7.2.1 Create and Maintain Change Management Process

Contractor shall be responsible for:

a. Complying with Government Change Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Change Management process.

7.2.2 Create and Record Request for Change (RFC)

Contractor shall be responsible for:

a. Determining type of change request that is required in accordance with Government Change Management Process
b. Determining change procedures to be used in accordance with Government Change Management Process.

c. Completing request for change form with required documentation in accordance with Government Change Management Process.

7.2.3 Review Request for Change (RFC)

a. Contractor shall be responsible for providing information for preliminary review of requests for change.

7.2.4 Assess and Evaluate Change

Contractor shall be responsible for:

a. Providing information to support impact assessment of requests for change.
b. Providing information to support categorization and risk assessment of requests for change
c. Providing information to support assessment of the benefit of implementing requests for change.

7.2.5 Authorize Change

Contractor shall be responsible for:

a. Obtaining Government authorization for changes to services or underlying infrastructure supporting services in accordance with Government Change Management Process.
b. Participating in Change Advisory Board(s) in accordance with Government Change Management Process.

7.2.6 Coordinate Change Implementation

Contractor shall be responsible for:

a. Developing change implementation procedures in accordance with Government Change Management Policy.
b. Coordinating activities with Government, I^3P Contractors and other Contractors to implement approved changes.

7.2.7 Review and Close Change Record

a. Contractor shall be responsible for providing information and participating in review meetings for closure of change records and capture of lessons learned.

7.3 Incident Management

7.3.0 High-Level Process Flow Diagram, Goal and General Provisions

Goal: The primary goal of Incident Management is to restore normal service operation as quickly as possible and minimize adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. "Normal service operation" is defined here as service operation within Service Level Agreement (SLA) limits.

Purpose: The purpose of Incident Management is to deal with all unplanned interruptions to an IT service or a reduction in the quality of IT service. This can include failures; questions or queries reported by users via telephone, email, or automatically detected and reported by event monitoring tools.

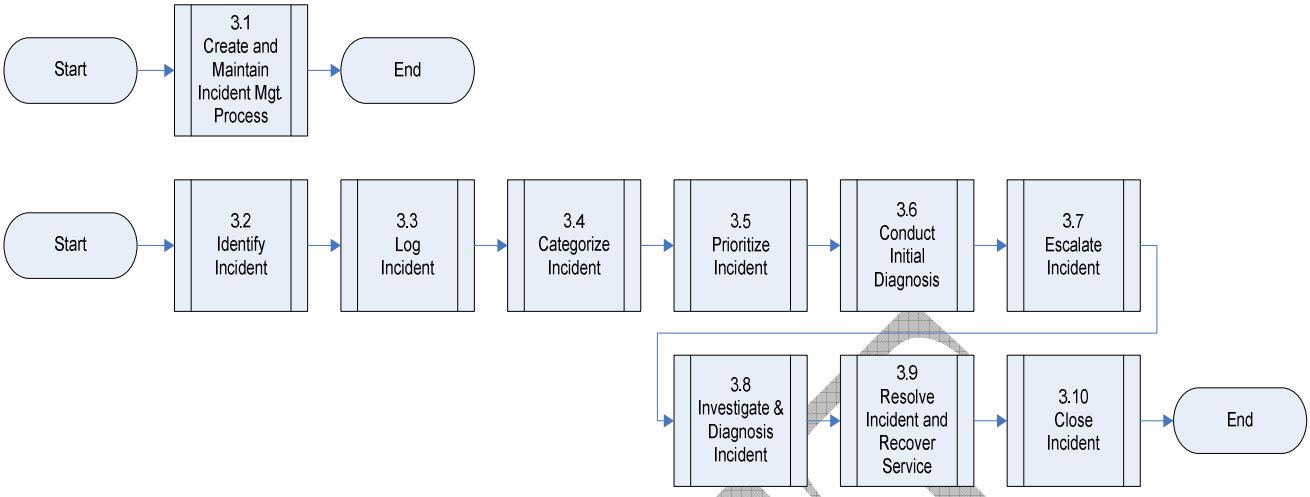


Figure 7: High-Level Incident Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for:

a. Designing and implementing Incident Management procedures that align with Government Incident Management Process.
b. Documenting, tracking and managing all Incidents using a Contractor or Government provided Incident Management system.
c. (When Contractors use a Contractor Incident Management System) Providing integration between Contractor and Government Incident Management systems including the integration of applicable software, e-mail and telephony in accordance with Government Incident Management Process. All changes necessary to provide system integration shall be made at Contractor expense. Contractor solution shall provide an efficient transfer of information between systems in accordance with DRD 1293CF-011, *Interface Definition Agreement (IDA)*.
d. Providing communications to users via Enterprise Service Desk and maintaining regular communications between all parties through Incident resolution in accordance with Government Incident Management Process.
e. Providing case ownership of Incidents that are assigned to Contractor until service is restored or ownership is reassigned.
f. Retaining ownership of each Incident assigned to Contractor by either the Enterprise Service Desk or Government Service Integration Management (SIM) office.
g. Assigning end-to-end responsibility of each Incident to a single point of contact in order to facilitate communications with Government until service is restored.
h. Resolving assigned Incidents in collaboration and coordination with Government, I^3P Contractors and other Contractors, and in accordance with Government Incident Management Process.
i. Complying with Government notification and escalation procedures in accordance with Government Incident Management Process.
j. Participating in daily Incident review meetings.

k. Implementing and supporting continuous improvement actions to reduce frequency and severity of reported Incidents.

7.3.1 Create and Maintain Incident Management Process

Contractor shall be responsible for:

a. Complying with Government Incident Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Incident Management process.

7.3.2 Identify Incident

Contractor shall be responsible for:

a. Detecting Incidents via both manual and automated monitoring mechanisms.
b. Notifying Enterprise Service Desk of an Incident within 15 minutes of detection.

7.3.3 Log Incident

Contractor shall be responsible for:

a. Logging Incidents in accordance with Government Incident Management Process.
b. Providing information to Enterprise Service Desk to ensure Incidents are logged in accordance with Government Incident Management Process.

7.3.4 Categorize Incident

Contractor shall be responsible for:

a. Categorizing Incidents in accordance with Government Incident Management Process.
b. Providing information to Enterprise Service Desk to ensure Incidents are categorized in accordance with Government Incident Management Process.

7.3.5 Prioritize Incident

Contractor shall be responsible for:

a. Prioritizing Incidents in accordance with Government Incident Management Process.
b. Providing information to Enterprise Service Desk to ensure Incidents are prioritized in accordance with Government Incident Management Process.

7.3.6 Conduct Initial Diagnosis

Contractor shall be responsible for:

a. Conducting initial diagnosis of Incidents in accordance with Government Incident Management Process.
b. Providing information to Enterprise Service Desk to ensure initial diagnosis of Incidents is performed in accordance with Government Incident Management Process.

7.3.7 Escalate Incident

Contractor shall be responsible for:

a. Providing Tier 2 and Tier 3 Incident resolution and support.
a. Accepting Incident Lead role as assigned.
a. Providing a mechanism for expedited handling of Incidents that are of high business priority to Government in accordance with Government Incident Management Process.
a. Opening 'Child' Incident records for other I^3P Contractor(s).
a. Providing status updates to Government Incident Management System.

7.3.8 Investigate and Diagnose Incident

Contractor shall be responsible for:

a. Conducting incident investigation and diagnostic activities to identify root cause and develop Incident work-around(s).
b. Executing Incident Management in accordance with Government Incident Management Procedures.

7.3.9 Resolve Incident and Recover Service

Contractor shall be responsible for:

a. Applying resolution or work around to restore service as quickly as possible.
b. Accomplishing resolution and recovery of all Incidents reassigned to Tier 2 and/or Tier 3 for support.
c. Notifying Enterprise Service Desk via Incident Management System that service is restored.
d. Recommending implementation of measures to avoid reoccurrence of Incidents relating to Services in accordance with Incident Management Procedures.

7.3.10 Close Incident

a. Contractor shall be responsible for providing Incident closure information in accordance with Government Incident Management Process.

7.4 Request Fulfillment

7.4.0 High-Level Process Flow Diagram and General Provisions

Goal: The goals of Request Fulfillment are: provide a channel for users to request and receive standard services for which a pre-defined approval and qualification process exists; provide information to users and customers about the availability of services and the procedure for obtaining them; source and deliver components of requested standard services; and assist with general information, complaints or comments.

Purpose: The purpose of Request Fulfillment is to deal with Service Requests from users whether small (i.e., low risk, frequently occurring, low cost (e.g. a request to change a password, a request to install additional software onto a particular workstation, and a request to relocate some items of a desktop)) or large – higher risk, less frequently occurring, higher cost (e.g. a request to replace major infrastructure or other service components or a request to refresh major software components)).

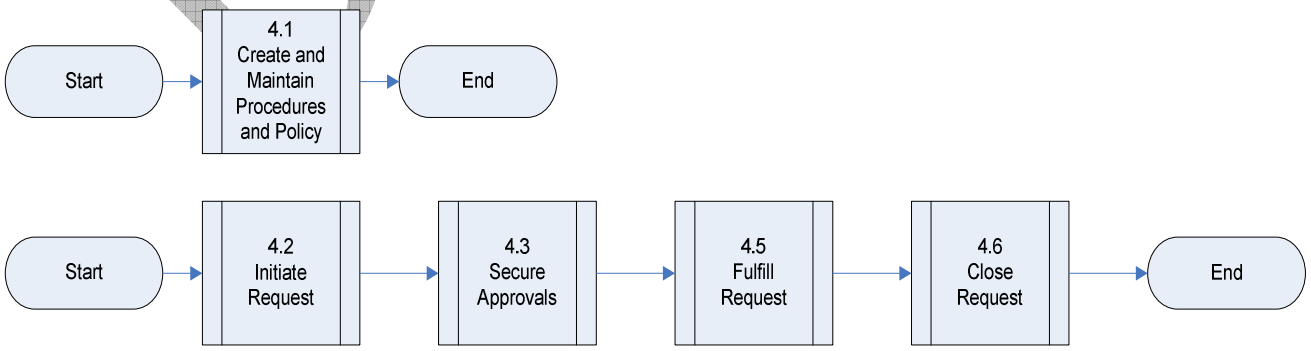


Figure 8: High-Level Request Fulfillment Process Flow Diagram

General Provisions:

Contractor shall be responsible for:

a. Designing and implementing Request Fulfillment procedures that align with Government Request Fulfillment Process.
b. Documenting, tracking and managing all Requests using a Contractor or Government provided Request Fulfillment system.
c. (When Contractors use a Contractor Request Fulfillment System) Providing integration between Contractor and Government Request Fulfillment systems including integration of applicable software, e-mail and telephony in accordance with Government Request Fulfillment Process. All changes necessary to provide system integration shall be made at Contractor expense. Contractor solution shall provide an efficient transfer of information between systems in accordance with DRD 1293CF-011, *Interface Definition Agreement (IDA)*.
d. Maintaining communications regarding Request status with users via Enterprise Service Desk from time a Request is identified, through closure and through any follow-up communication.
e. Providing case ownership of Requests that are assigned to Contractor until Request is closed.
f. Participating in Request Fulfillment review meetings.
g. Implementing and supporting continuous improvement of Request Fulfillment through self-service or other mechanisms.

7.4.1 Create and Maintain Request Fulfillment Process

Contractor shall be responsible for:

a. Complying with Government Request Fulfillment Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Request Fulfillment process.

7.4.2 Initiate Request

Contractor shall be responsible for:

a. Utilizing Government provided Enterprise Service Catalog to fulfill customer requests.
b. Providing a mechanism to receive non-standard requests from Request Fulfillment system in accordance with Government Request Fulfillment Process.

7.4.3 Secure Approvals

a. Contractor shall be responsible for providing supporting information on all standard and non-standard Requests in support of approvals in conformance with Government Request Fulfillment Process. Supporting information includes, but is not limited to, viable alternatives to fulfilling the Request, risk assessments, revised cost estimates, implementation timing, and dependencies.

7.4.4 Fulfill Request

Contractor shall be responsible for:

a. Fulfilling all standard Requests within Government Service Level Agreements as defined for each standard Request and in conformance with Government Request Fulfillment Process.
b. Fulfilling all non-standard Requests as mutually agreed and in accordance with Government Request Fulfillment Process.

c. Enabling fulfillment of a Request in collaboration and coordination with Government, I[3]P Contractors and other Contractors and in accordance with Government Request Fulfillment Process.
d. Providing accurate and regular status updates for all Requests assigned to Contractor in accordance with Government Request Fulfillment Process.

7.4.5 Close Request

a. Contractor shall be responsible for providing Request closure information in accordance with Government Request Fulfillment Process.

7.5 Problem Management

7.5.0 High-Level Process Flow Diagram and General Provisions

Goal: The primary goals of Problem Management are: to prevent problems and resulting Incidents from happening, to eliminate recurring Incidents and to minimize the impact of Incidents that cannot be prevented.

Purpose: The purpose of Problem Management is to provide a pre-defined and approved process for managing the lifecycle of all Problems to include diagnosis, determination of resolutions to those Problems, implementing solutions through appropriate control and change management procedures and preventing Problem reoccurrence.

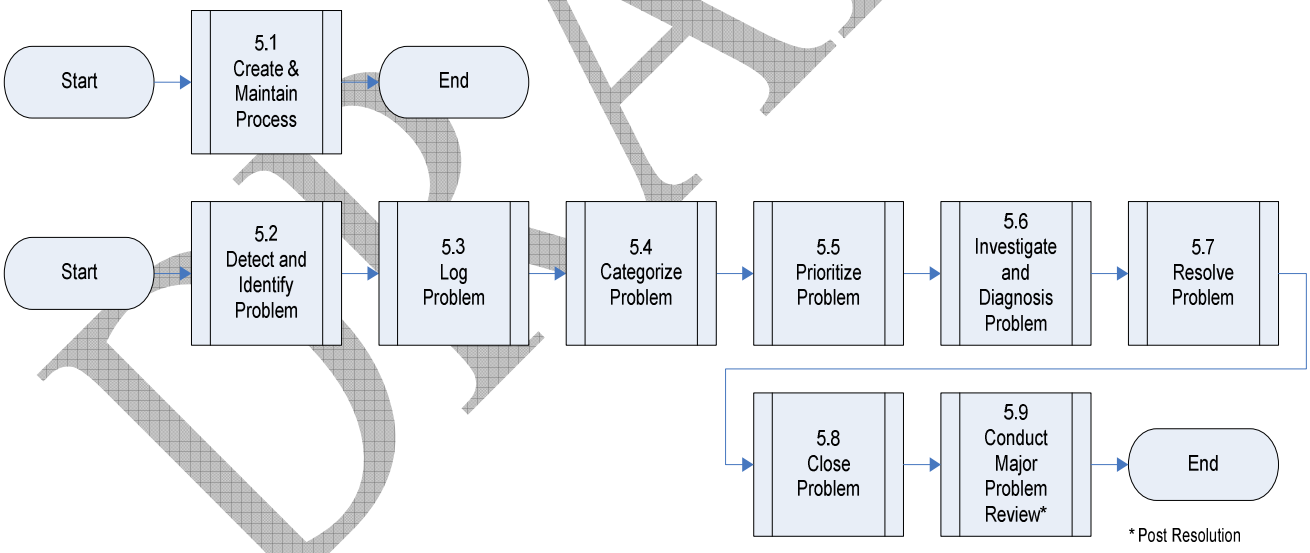


Figure 9: High-Level Problem Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for:

a. Designing and implementing Problem Management procedures that align with Government Problem Management Process.
a. Documenting, tracking and managing all Problems in a Government Problem Management System.

a. (When Contractors use a Contractor Problem Management System) Providing integration between Contractor and Government Problem Management systems including integration of applicable software, e-mail and telephony in accordance with Government Problem Management Process. All changes necessary to provide system integration shall be made at Contractor expense. Contractor solution shall provide an efficient transfer of information between systems in accordance with DRD 1293CF-011, *Interface Definition Agreement (IDA)*.
d. Retaining ownership of each problem assigned to Contractor by either Enterprise Service Desk or Government Service Integration Management (SIM) office.
    1) To the extent a Problem does not arise from or relate to the Contractor's Services:
        i. The Contractor shall notify Enterprise Service Desk in accordance with Government Problem Management Procedures.
        ii. The Contractor shall maintain responsibility for the Problem until the Problem is reassigned by Enterprise Service Desk or Government Service Integration Management (SIM) office.
e. Assigning end-to-end responsibility of each Problem to a single point of contact in order to facilitate communications with Government.
f. Monitoring, controlling and managing each Problem assigned to Contractor until it is closed by Enterprise Service Desk.
g. Resolving assigned Problems in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with Government Problem Management Process.
h. Complying with Government notification and escalation procedures in accordance with Government Problem Management Process.

7.5.1 Create and Maintain Problem Management Process

Contractor shall be responsible for:

a. Complying with Government Problem Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Problem Management process.

7.5.2 Detect and Identify Problem

Contractor shall be responsible for:

a. Identifying Problems by proactively performing on-going trend analysis on Incident information.
b. Detecting Problems via both manual and automated monitoring mechanisms.

7.5.3 Log Problem

Contractor shall be responsible for:

a. Logging Problems in accordance with Government Problem Management Process.
b. Providing information to Enterprise Service Desk to ensure Problems are logged in accordance with Government Problem Management Process.

7.5.4 Categorize Problem

Contractor shall be responsible for:

a. Categorizing Problems in accordance with Government Problem Management Process.
b. Providing information to Enterprise Service Desk to ensure Problems are categorized in accordance with Government Problem Management Process.

7.5.5 Prioritize Problem

Contractor shall be responsible for:

a. Prioritizing Problems in accordance with Government Problem Management Process.
b. Providing information to Enterprise Service Desk to ensure Problems are prioritized in accordance with Government Problem Management Process.

7.5.6 Investigate and Diagnose Problem

Contractor shall be responsible for:

a. Conducting Problem investigation in accordance with Government Problem Management Process.
b. Conducting Problem diagnostics in accordance with Government Problem Management Procedures.
c. Providing status tracking information in Government Problem Management System in accordance with Government Problem Management Process.
d. Investigating and diagnosing Problems in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with Government Problem Management Process.
e. Validating Problem workarounds.
f. Providing communications to users via Enterprise Service Desk and maintaining regular communications between all parties through Problem resolution in accordance with Government Problem Management Process.
g. Performing Root Cause Analysis (RCA) in accordance with Government Problem Management Procedures.
h. Updating Known Error information in accordance with Government Problem Management Process
i. Documenting problem resolution in accordance with Government Problem Management Process.
j. Developing a Corrective Action Plan in accordance with Government Problem Management Process.

7.5.7 Resolve Problem

Contractor shall be responsible for:

a. Determining if initiation of Change Management Process is required.
b. Generating requests for change for permanent solutions and corrective action plans in accordance with Government Change Management Process.
c. Applying resolutions across the enterprise, as applicable.
d. Implementing the approved corrective action plan with follow-up to eliminate the fault from the operating environment.
e. Resolving Problems in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with Government Problem Management Process..
f. Developing diagnostic scripts for Enterprise Service Desk to facilitate resolution of repetitive problems.

7.5.8 Close Problem

a. Contractor shall be responsible for Providing Problem resolution and closure information in Government Problem Management System in accordance with Government Problem Management Process.

7.5.9 Conduct Major Problem Review

Contractor shall be responsible for:

a. Participating in major Problem reviews.

b. Providing Problem resolution details.

7.6 Service Level Management (SLM)

7.6.0 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Service Level Management is to ensure that an agreed upon level of service is provided for all IT services, and that future services are delivered in accordance with Service Level Agreements. Proactive measures are also taken to seek and implement improvements to the level of service delivered.

Purpose: The purpose of Service Level Management is to ensure that all operational services and their performance are managed in a consistent manner throughout the IT organization to meet the needs of the business and customers.

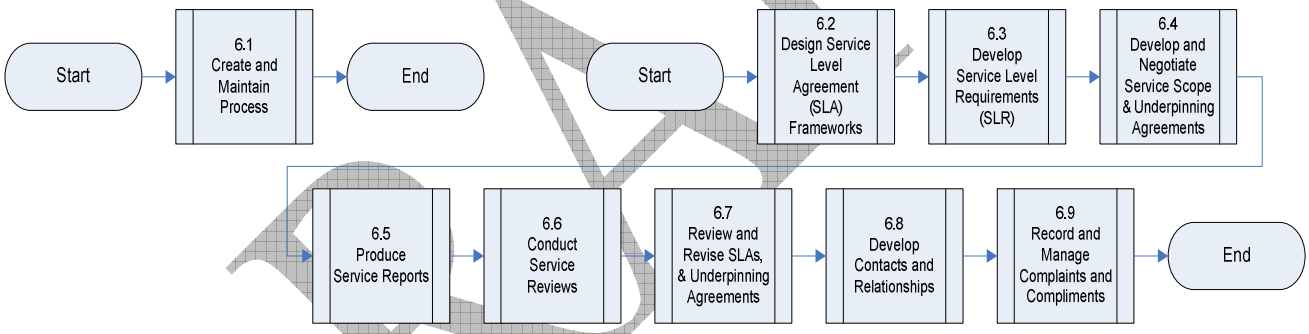


Figure 10: High-Level Service Level Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for designing and implementing SLM procedures that align with Government SLM Process.

7.6.1 Create and Maintain SLM Process

Contractor shall be responsible for:

a. Complying with the approved Government SLM Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government SLM process.

7.6.2 Design Service Level Agreement (SLA) Frameworks

a. Contractor shall be responsible for providing information to support design and development of Service Level Agreement frameworks .

7.6.3 Develop Service Level Requirements (SLR)

a. Contractor shall be responsible for providing information to support Government with developing Service Level Requirements and gaining agreement with Government IT services customers.

7.6.4 Develop and Negotiate Service Level Scope and UnderpinningAgreements

a. Contractor shall be responsible for providing information to support Government with developing and drafting service level scope and underpinning agreements.

7.6.5 Produce Service Level Reports

a. Contractor shall be responsible for providing information to support Government reporting of Service Levels in accordance with Government SLM Process.

7.6.6 Conduct Service Reviews

a. Contractor shall be responsible for supporting Government service reviews (e.g., meetings) in accordance with Government SLM Process.

7.6.7 Review and Revise Service Level Agreements and Underpinning Agreements

a. Contractor shall be responsible for providing information to support Government with reviewing and revising Service Levels and underpinning agreements.

7.6.8 Develop Contacts and Relationships

a. Contractor shall be responsible for providing information to support Government with developing customer relationships as it relates to IT services, service performance, and service agreements.

7.6.9 Record and Manage Customer Service Level Feedback

Contractor shall be responsible for:

a. Providing information to Enterprise Service Desk regarding customer Service Level feedback in accordance with Government SLM Process.
b. Providing information to support Government with assigning and dispositioning actions related to customer feedback.

7.7 Service Asset and Configuration Management (SACM)

7.7.0 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goals of SACM are to: support the business and customer's control objectives and requirements; support efficient and effective Service Management processes by providing accurate configuration information to enable people to make decisions at the right time (e.g., to authorize change and releases and to resolve incidents and problems faster); minimize the number of quality and compliance issues caused by improper configuration of services and assets; and optimize service assets, IT configurations, capabilities and resources.

Purpose: The purpose of SACM is to: identify, control, record, report, audit and verify Service Assets and Configuration Items, including versions, baselines, constituent components, and their attributes and relationships; account for, manage, and protect the integrity of Service Assets and Configuration Items (and where appropriate, those of their customers) throughout the service lifecycle.

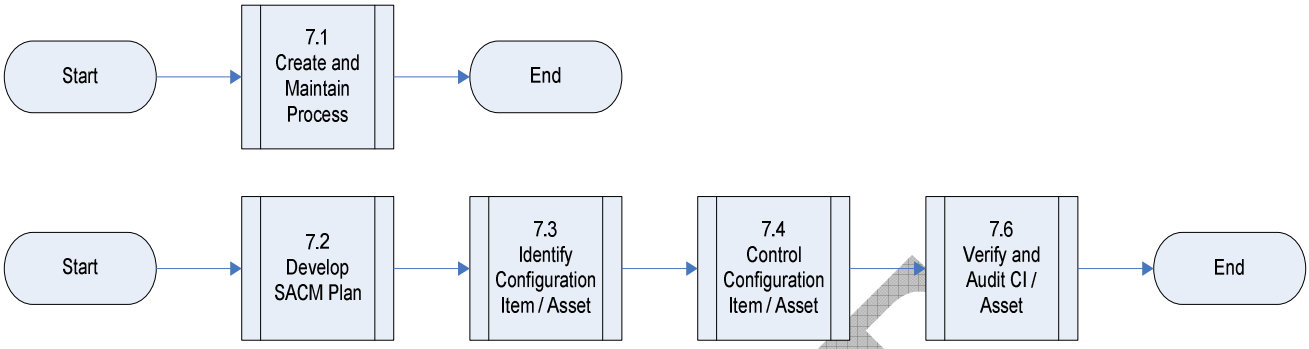


Figure 11: High-Level Service Asset and Configuration Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for:

a. Defining and implementing Contractor SACM procedures in accordance with Government SACM Process.
b. Documenting, tracking and managing all Service Assets and Configuration Items in Government CMDB in accordance with Government SACM Process.
c. (When Contractors use a Contractor CMDB System) Providing integration between Contractor and Government CMDB systems including integration of applicable software, e-mail and telephony in accordance with Government SACM Process. All changes necessary to provide system integration shall be made at Contractor expense. Contractor solution shall provide an efficient transfer of information between systems in accordance with DRD 1293CF-011, *Interface Definition Agreement (IDA)*.

7.7.1 Create and Maintain Service Asset and Configuration Management (SACM) Process

Contractor shall be responsible for:

a. Complying with Government SACM Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government SACM process.

7.7.2 Develop Service Asset and Configuration Management (SACM) Plan

a. Contractor shall be responsible for developing and maintaining SACM Plan in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with DRD 1293CF-003, *Service Asset and Configuration Management (SACM) Plan*.

7.7.3 Identify Configuration Item / Asset

Contractor shall be responsible for:

a. Developing a strategy for ensuring identification of all Configuration Items in accordance with Government SACM Process.
b. Identifying and labeling, as applicable, all Configuration Items in accordance with Government SACM Process
c. Assigning unique identifiers to each Configuration Item in accordance with Government SACM Process.
d. Specifying relevant attributes, relationships, owner and baselines for each Configuration Item in accordance with Government SACM Process.

7.7.4 Control Configuration Item / Asset

Contractor shall be responsible for:

a. Identifying when a change to a Configuration Item is necessary and initiating a request for change in accordance with Government Change Management Process.
b. Determining and reporting the root cause, impact, and actions to prevent recurrence of an unauthorized change in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with Government SACM Process.

7.7.5 Verify and Audit Configuration Item / Asset

Contractor shall be responsible for:

a. Participating in Government audit activities to ensure conformity between documented Configuration Items and actual Configuration Items in accordance with Government SACM Process.
b. Providing audit Configuration Item data and Release documentation in accordance with Government SACM Process.
c. Implementing corrective actions in accordance with Government SACM Process.
d. Providing information to support audit reporting in accordance with Government SACM Process.

7.8 RELEASE AND DEPLOYMENT MANAGEMENT (RDM)

7.8.0 High Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Release and Deployment Management is to deploy releases into production and establish effective use of the service.

Purpose: The purpose of Release and Deployment Management is to: define and agree on release and deployment plans with customers and stakeholders; ensure that integrity of a release package and its constituent components is maintained throughout the transition activities and recorded accurately in the Configuration Management Database (CMDB); ensure that all release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out if appropriate; and ensure that customers and stakeholder change is managed during Release and Deployment activities.

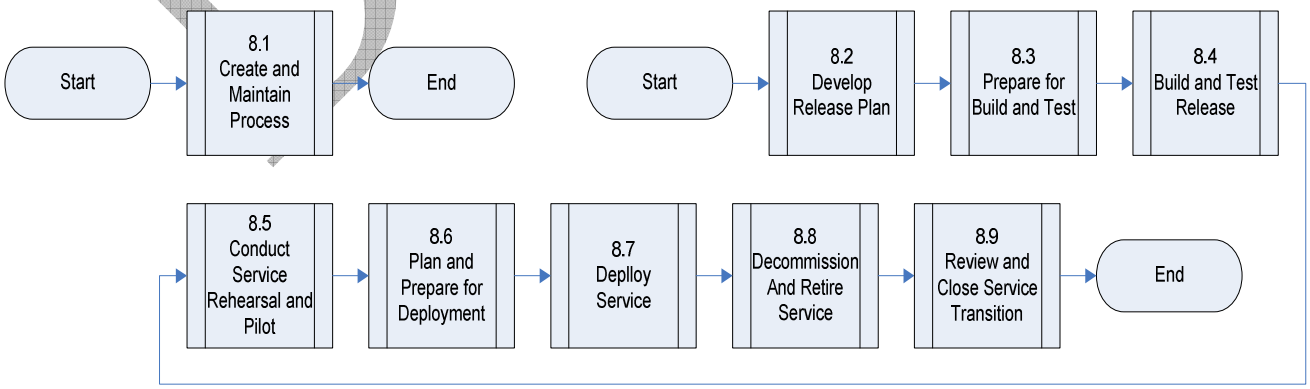


Figure 12: High-Level Release and Deployment Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for performing Releases in accordance with Government Release and Deployment Process.

7.8.1 Create and Maintain Release and Deployment Management Process

Contractor shall be responsible for:

a. Complying with Government RDM Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government RDM Process.
c. Conducting an annual inventory of applications being used to support NASA services, and report this data, including the cost to develop, operate, enhance and maintain applications as specified in DRD 1293CF-005, *Application Inventory (AI) Report*.
d. Reviewing NASA Enterprise Architecture Repository (NEAR) to verify if an existing application can fulfill requirements prior to purchasing or developing a new capability or application.

7.8.2 Develop Release Plan

a. Contractor shall be responsible for developing and maintaining RDM Plan in collaboration and coordination with Government, I^3P Contractors , and other Contractors and in accordance with DRD 1293CF-004, *Release and Deployment Management (RDM) Plan*.

7.8.3 Prepare for Release Build and Test

a. Contractor shall be responsible for preparing for release build and test in collaboration and coordination with Government, I^3P Contractors and other Contractors.

7.8.4 Build and Test Release

Contractor shall be responsible for:

a. Building and testing releases in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with Government RDM Process.
b. Developing release documentation in accordance with Government RDM Process.
c. Creating test scenario and acceptance criteria and submitting them for review in accordance with Government RDM Process.
d. Managing Release build and test environments.

7.8.5 Conduct Service Rehearsal and Pilot

a. Contractor shall be responsible for conducting service rehearsals and pilots in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with Government RDM Process.

7.8.6 Plan and Prepare for Deployment

Contractor shall be responsible for:

a. Planning and preparing for deployment in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with Government RDM Process.
b. Assessing the need for and planning for a release stabilization period in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with Government RDM Process.

7.8.7 Deploy Service

Contractor shall be responsible for:

a. Deploying services in collaboration and coordination with Government, I^{3}P Contractors and other Contractors and in accordance with Government RDM Process.
b. Verifying successful service deployment in collaboration and coordination with Government, I^{3}P Contractors and other Contractors and in accordance with Government RDM Process.
c. Executing back-out plan, if necessary, in collaboration and coordination with Government, I^{3}P Contractors and other Contractors and in accordance with Government RDM Process.

7.8.8 Decommission and Retire Service

a. Contractor shall be responsible for decommissioning and retiring services in collaboration and coordination with Government, I^{3}P Contractors and other Contractors and in accordance with Government RDM Process.

7.8.9 Review and Close Service Release Deployment

a. Contractor shall be responsible for closing release deployment in accordance with Government RDM Process.

7.9 CAPACITY MANAGEMENT

7.9.0 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Capacity Management process is to ensure IT capacity in all areas of IT is matched to the needs of the Government's business.

Purpose: The purpose of Capacity Management is to provide a point of focus and management for all capacity and performance related issues, relating to both services and resources.

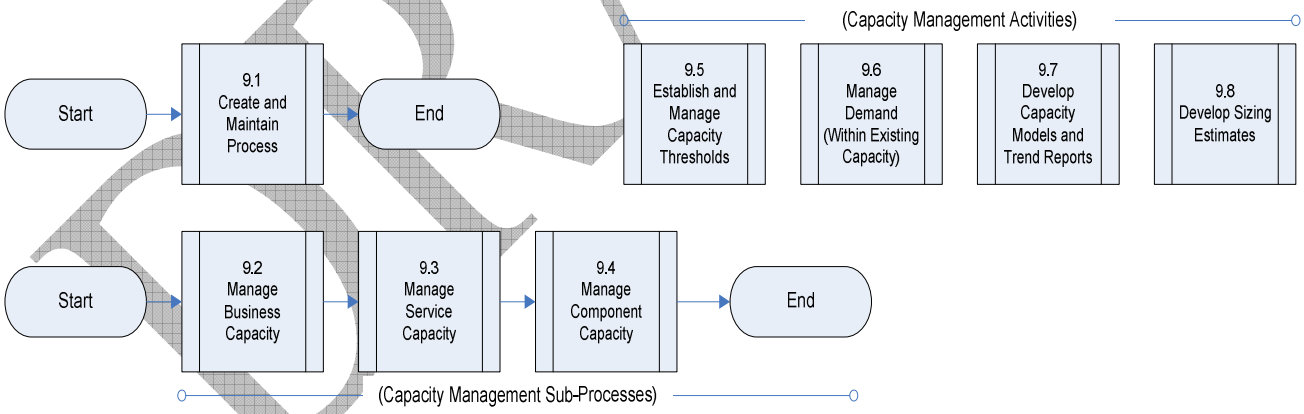


Figure 13: High-Level Capacity Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for:

a. Designing and implementing Capacity Management procedures that align with Government Capacity Management Process.

b. Developing and maintaining Capacity Management Plan in collaboration and coordination with Government, I^{3}P Contractors, and other Contractors and in accordance with DRD 1293CF-006, *Capacity Management Plan*.
c. Conducting annual reviews of projected capacity requirements for infrastructure and related services, and providing recommendations based upon information provided by Government Portfolio Management Process as part of Government's normal business planning cycle.

7.9.1 Create and Maintain Capacity Management Process

Contractor shall be responsible for:

a. Complying with Government Capacity Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Capacity Management Process.

7.9.2 Manage Business Capacity

Contractor shall be responsible for:

a. Providing impact assessment of potential business capacity issues based on Government business direction.
b. Prototyping and sizing capacity impact solutions, including:
    1) Developing and maintaining standard templates for capacity test plans in collaboration and coordination with Government, I^{3}P Contractors and other Contractors.
    2) Coordinating tests with Government, I^{3}P Contractors and other Contractors to provide end-to-end testing.
    3) Testing and sizing models for capacity impacts.
c. Developing plans for required changes to existing capacity in accordance with DRD 1293CF-006, *Capacity Management Plan*.

7.9.3 Manage Service Capacity

Contractor shall be responsible for:

a. Providing Service Manager with information regarding Service Capacity and issues.
b. Monitoring Service Capacity including:
    1) Collecting Service Capacity performance data, at a minimum, per the following schedule:
        i. Daily data collection for volatile and dynamic systems.
        ii. Weekly data collection for variable and stable systems.
    2) Maintaining Services aligned with Government Enterprise Service Catalog.
c. Analyzing Service Capacity, including:
    1) Providing service capacity performance reports in accordance with DRD 1293CF-007, *Service and Component Capacity Report*.
d. Tuning Service performance, including changing capacity, to take corrective action or adjust for more effective usage.
e. Establishing capacity thresholds and making adjustments based on Government requirements.
f. Responding to Government requests for capacity impact statements within 30 days.

7.9.4 Manage Component Capacity

Contractor shall be responsible for:

a. Providing Service Manager with information regarding component capacity and issues.
b. Monitoring component capacity usage, including:

1) Maintaining components aligned with Government Enterprise Service Catalog.

c. Analyzing component usage, including:
   1) Reviewing component capacity data.
   2) Determining if proactive changes are needed.
   3) Determining if tuning or replacing a component can provide for a more effective use of the component.
d. Tuning or replacing components, including:
   1) Adjusting or balancing component capacity to provide more effective usage.
   2) Changing component capacity to correct utilization issues.
   3) Replacing components in compliance with Change Management Process.
   4) Collecting and providing component capacity data based on Government-specified standards and metrics.
e. Providing component capacity reports in accordance with DRD 1293CF-007, *Service and Component Capacity Report*.
f. Reviewing, validating and updating component baselines and profiles in the CMDB.

7.9.5 Establish and Manage Capacity Thresholds

a. Contractor shall be responsible for monitoring and generating alerts and warnings associated with capacity and performance thresholds.

7.9.6 Manage Demand (within existing capacity)

a. Contractor shall be responsible for providing information and support to manage demand within existing capacity levels.

7.9.7 Develop Capacity Models and Trend Reports

a. Contractor shall be responsible for providing capacity models and trend reports in accordance with DRD 1293CF-007, *Service and Component Capacity Report*.

7.9.8 Develop Sizing Estimates

a. Contractor shall be responsible for developing sizing estimates to support capacity planning.

7.10 Availability Management

7.10.0 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The Goal of Availability Management is to ensure that the level of service availability delivered in all services is matched to the requirements of the Government's business.

Purpose: The Purpose of Availability Management is to provide a point of focus and management for all availability-related issues, relating to both services and resources, ensuring that availability targets in all areas are measured and achieved.

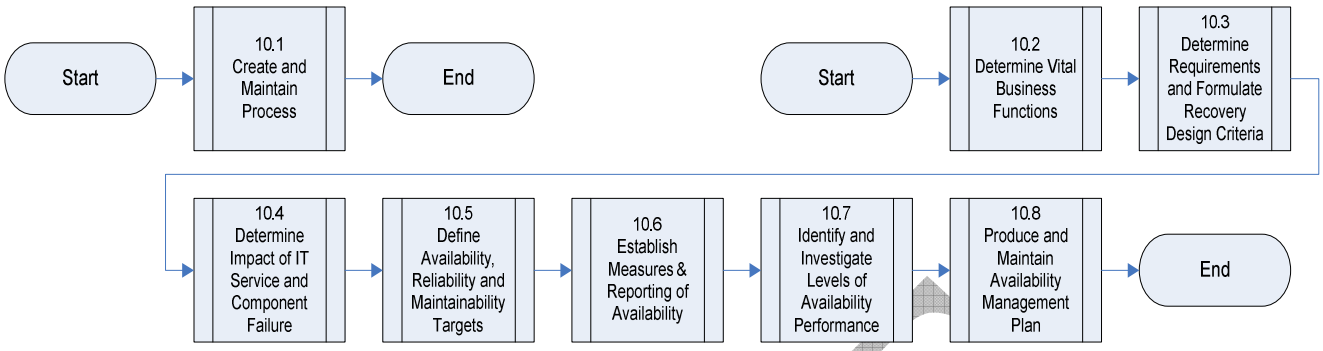


Figure 14: High-Level Availability Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for designing and implementing Availability Management procedures that align with Government Availability Management Process.

Identifying planned downtime and scheduling downtime in collaboration and coordination with Government, I^{3}P Contractors and other Contractors and in alignment with Government Mission Flight Requirements.

7.10.1 Create and Maintain Availability Management Process

Contractor shall be responsible for:

a. Complying with Government Availability Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Availability Management Process.

7.10.2 Determine Vital Business Functions

a. Contractor shall be responsible for providing information to support Government with identifying vital business functions.

7.10.3 Determine Requirements and Formulate Recovery Design Criteria

a. Contractor shall be responsible for providing information to support Government with defining availability requirements.
b. Providing information to support Government with formulating recovery design criteria

7.10.4 Determine Impact of IT Service and Component Failure

a. Contractor shall be responsible for providing information to support Government with conducting business and service impact analysis and component failure impact analysis related to availability.

7.10.5 Define Availability, Reliability and Maintainability Targets

a. Contractor shall be responsible for providing information to support Government with developing and maintaining availability, reliability and maintainability targets and measures that align with applicable Service Level Agreements.

7.10.6 Monitor and Analyze Availability, Reliability and Maintainability

Contractor shall be responsible for:

a. Establishing service metrics and tools for measuring availability, reliability and maintainability in accordance with Government Availability Management Process.

b. Deploying tool sets and/or interfaces to permit end-to-end measurement of availability.
c. Collecting and recording availability, reliability and maintainability data.
d. Monitoring availability, reliability and maintainability elements with respect to Service Levels.
e. Conducting analysis for compliance with availability, reliability and maintainability Service Levels.
f. Reporting results of monitoring and analysis in accordance with DRD 1293CF-009, *Availability, Reliability, and Maintainability (ARM) Analysis Report*.
g. Providing information to assist in Problem analysis related to service availability.

7.10.7 Identify and Investigate Levels of Availability Performance

Contractor shall be responsible for:

a. Identifying Availability performance that fails to meet Government Service Level Agreements.
b. Investigating availability performance that fails to meet Government Service Level Agreements.
c. Initiating actions to ensure availability performance complies with Government Service Level Agreements.

7.10.8 Produce and Maintain Availability Management Plan

Contractor shall be responsible for:

a. Developing and maintaining Availability Management Plan in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with DRD 1293CF-008, *Availability Management (AM) Plan*.
b. Addressing end-to-end availability requirements in any designs to ensure compliance with Government design and architecture standards.
c. Addressing end-to-end availability requirements in defining and executing any test plans.
d. Identifying planned downtime and scheduling downtime in collaboration and coordination with Government, I^3P Contractors and other Contractors and in accordance with applicable Service Level Agreements.
e. Implementing requested changes to availability metrics and Service Level Agreement in accordance with Government SLM Process.

7.11 IT SERVICE CONTINUITY MANAGEMENT (ITSCM)

7.11.0 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of ITSCM is to support the overall Business Continuity Management process by ensuring that required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required business timeframes.

Purpose: The purpose of ITSCM is to establish and maintain required ongoing recovery capability within required IT services and their supporting components.

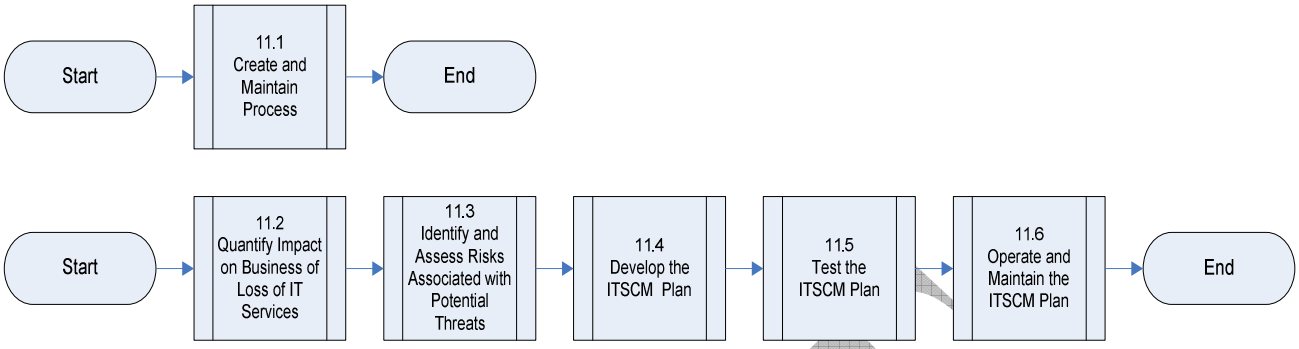


Figure 15: High-Level IT Service Continuity Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for:

a. Designing and implementing ITSCM Management procedures that align with Government ITSCM Process.
b. Providing ITSCM Services to mitigate the impact of a disaster or major failure in accordance with Government ITSCM Process.
c. Developing, documenting and maintaining procedures (e.g., Disaster Recovery checklists) in collaboration and coordination with Government, I^{3}P Contractors and other Contractors to meet Government requirements (e.g., Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)).

7.11.1 Create and Maintain IT Service Continuity Management Process

Contractor shall be responsible for:

a. Complying with Government ITSCM Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government ITSCM process.

7.11.2 Quantify Impact on Business of Loss of IT Services

Contractor shall be responsible for:

a. Providing information to support analysis of the impact of continuity scenarios.
b. Providing information to support identification and impact of contingency options and mitigation actions.

7.11.3 Identify and Assess Risks Associated with Potential Threats

Contractor shall be responsible for:

a. Providing information to support identification of risk responses and proposed countermeasures.
b. Participating in IT risk assessment activities in order to reduce vulnerability to the business.

7.11.4 Develop the IT Service Continuity Management (ITSCM) Plan

Contractor shall be responsible for:

a. Developing and maintaining ITSCM Plan in collaboration and coordination with Government, I^{3}P Contractors and other Contractors and in accordance with DRD 1293CF-010, *Information Technology (IT) Service Continuity Management (ITSCM) Plan*.

b. Supporting business criticality classification in accordance with Government Enterprise Service Catalog.

7.11.5 Test the IT Service Continuity Management (ITSCM) Plan

Contractor shall be responsible for:

a. Developing test scenarios in collaboration and coordination with Government, I^3P Contractors and other Contractors in support of conducting testing of ITSCM Plan in accordance with Government ITSCM Process.
b. Conducting walkthrough, full, partial and scenario tests in accordance with Government ITSCM Process.

7.11.6 Operate and Maintain the ITSCM Plan

Contractor shall be responsible for:

a. Participating in Government ITSCM reviews in accordance with Government ITSCM Process.
b. Invoking ITSCM plan in accordance with Government ITSCM Process.
c. Performing training functions including:
   1) Developing and updating Contractor ITSCM training plans and material.
   2) Training Contractor recovery team members.
d. Maintaining local work procedures and contact lists.
e. Performing ITSCM Plan gap analysis and response planning and updating Contractor ITSCM Plan accordingly.
f. Documenting all contingency services provided in Government Service Level Agreements.
g. Executing recovery plans and restoring Service to normal operation.
h. Supporting ITSCM evaluation efforts following disaster events, including providing evaluations and lessons learned and updating Contractor ITSCM Plan as needed.

7.12 Knowledge Management

7.12.0 High-Level Process Flow Diagram, Goal, Purpose and General Provisions

Goal: The goal of Knowledge Management is to enable organizations to improve the quality of management decision making by ensuring that reliable and secure information and data is available throughout the service lifecycle.

Purpose: The purpose of Knowledge Management is to ensure that the right information is delivered to the appropriate place or person at the right time to enable informed decision making.

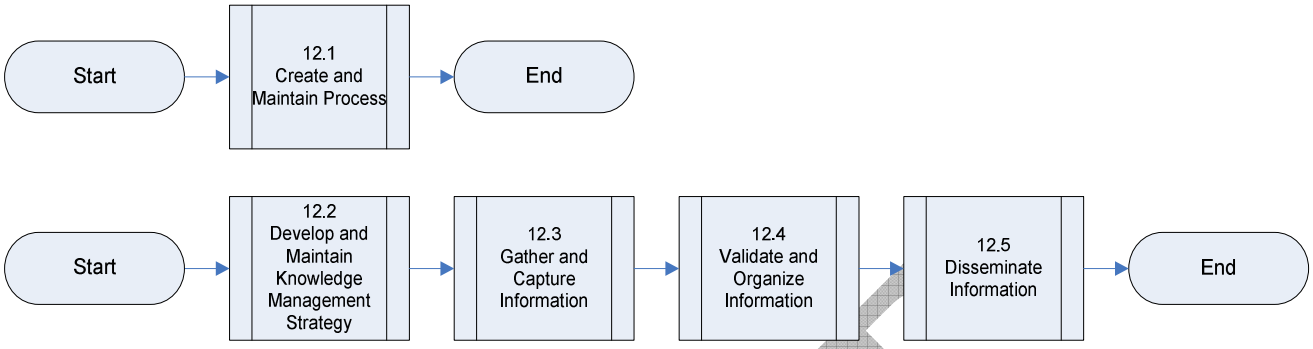


Figure 16: High-Level Knowledge Management Process Flow Diagram

General Provisions:

Contractor shall be responsible for:

a. Designing and implementing knowledge management procedures and tools to support knowledge capture and dissemination in accordance with Government Knowledge Management Process.
b. Managing and maintaining knowledge and information assets in collaboration and coordination with Government, I³P Contractors and other Contractors, and in accordance with Government Knowledge Management Process.

7.12.1 Create and Maintain Knowledge Management Process

Contractor shall be responsible for:

a. Complying with Government's Knowledge Management Process.
b. Performing continuous analysis of industry best practices or trends and inform Government of changes that could impact or improve Government Knowledge Management process.

7.12.2 Develop and Maintain Knowledge Management System

a. Contractor shall be responsible for providing Government with information to support development and maintenance of the Knowledge Management system.

7.12.3 Gather and Capture Information

a. Contractor shall be responsible for gathering and capturing information in accordance with Government Knowledge Management Process.

7.12.4 Validate and Organize Information

a. Contractor shall be responsible for validating and organizing information in accordance with Government Knowledge Management Process.

7.12.5 Disseminate Information

a. Contractor shall be responsible for disseminating information in accordance with Government Knowledge Management Process.

7.13 Information Security Management (ISM)

7.13.0 High-Level Process Flow Diagram, Goal and Purpose

Goal: The goal of ISM is to align IT security with business security and ensure that information security is effectively managed across all service management and service delivery activities.

Purpose: The purpose of ISM is to provide a point of focus and management for all aspects of IT security.

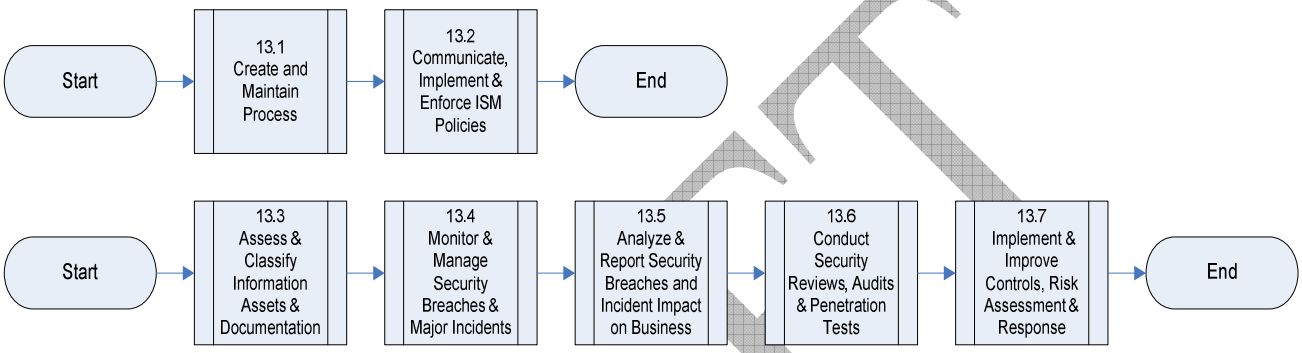


Figure 17: High-Level Information Security Management Process Flow Diagram

7.13.1 Create and Maintain Information Security Management (ISM) Process

Contractor shall be responsible for:

a. Complying with Government's ISM policies and procedures. Examples include Federal Information Security Management Act (FISMA) and National Institute of Standards and Technology (NIST). See Section 6, Common Information Technology Security Requirements, in this document.
b. Performing continuous analysis of industry best practices or trends and informing Government of changes that could impact or improve Government ISM process.

7.13.2 Communicate, Implement and Enforce Information Security Management (ISM) Procedures

Contractor shall be responsible for:

a. Implementing Government ISM policies (e.g., FISMA) for all Contractor services provided.
b. Supporting Government's ISM policy enforcement efforts and providing details of Information security practices to Government.

7.13.3 Assess and Classify Information Assets and Documentation

Contractor shall be responsible for:

a. Providing information to Government to support information asset identification and documentation in accordance with Government's ISM policy.
b. Providing information to Government to support information asset review activities regarding completeness, accuracy, and vulnerability.
c. Providing information to Government to support classification of information assets in accordance with Government's ISM policy.

7.13.4 Monitor and Manage Security Breaches and Major Incidents

Contractor shall be responsible for:

a. Monitoring and reporting security breaches and security incidents in accordance with Government's ISM procedures.
b. Providing information to Government to support investigation of any security breach and/or security Incident.
c. Providing information to Government to support resolution of any security breach and/or security Incident.

7.13.5 Analyze and Report Security Breaches and Incident Impact on Business

a. Contractor shall be responsible for participating in review and analysis of security breaches and security Incidents and providing detailed information to Government to support analysis of business impact and creation of security breach and security Incident report.

7.13.6 Conduct Security Reviews, Audits and Penetration Tests

Contractor shall be responsible for:

a. Conducting security reviews and regular audits of information and technology assets under Contractor's control in accordance with Government's ISM policy.
b. Participating in periodic Government security audits as requested by Government and coordinating audit activities of Third Parties as required or requested by Government.
c. Conducting and supporting security penetration testing as required or when requested by Government in accordance with Government's ISM policy.

7.13.7 Improve Security Controls, Risk Assessment and Responses

Contractor shall be responsible for:

a. Providing information to Government to support the assessment of security risks.
b. Participating in development and maintenance of security improvement plans in accordance with Government's ISM policy.

8 Glossary of Terms

Activity	A set of actions designed to achieve a particular result. Activities are usually defined as part of Processes or plans, and are documented in procedures.
Asset	Any resource or capability. Assets of a Contractor include anything that could contribute to the delivery of a service. Assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.
Asset Management	Asset Management is the Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process.
Availability	The ability of a Configuration Item or IT Service to perform its agreed function when required.
Availability Management	The Process responsible for defining, analyzing, planning, measuring and improving all aspects of the availability of IT Services. Availability Management is responsible for ensuring that all IT infrastructure, Processes, tools, roles etc are appropriate for the agreed Service Level Targets for availability.
Capacity	The maximum throughput that a Configuration item or IT Service can deliver while meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.
Capacity Management	The Process responsible for ensuring that the capacity of IT Services and the IT infrastructure is able to deliver agreed Service Level Targets in a cost effective and timely manner. Capacity Management considers all resources required to deliver the IT Service and plans for short, medium and long term business requirements.
Change	The addition, modification or removal of anything that could have an effect on IT Services. The scope of any Change should include all IT Services, Configuration Items, Processes, documentation etc.
Change Management	The Process responsible for controlling the Lifecycle of all changes. The primary objective of Change Management is to enable beneficial changes to be made with minimum disruption to IT Services.
Component	A general term used to mean one part of something more complex. For example, a computer system may be a Component of an IT Service; an Application may be a Component of a Release unit. Components that are managed as part of an IT Service should be Configuration Items and managed as part of the enterprise Configuration Management Process.

Configuration Item (CI)	Any component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a configuration record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people and formal documentation such as Process documentation and SLAs.
Configuration Management	The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their relationships. This information is managed throughout the Lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.
Continual Service Improvement	A stage in the Lifecycle of an IT Service. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services.
Contractor Management	The Process responsible for ensuring that all Contracts with Contractors support the needs of the business, and that all Contractors meet their contractual commitments.
Customer	Someone who buys goods or services. The Customer of an IT Service Contractor is the person or group that defines and agrees the Service Level Targets.
Deployment	The Activity responsible for movement of new or changed hardware, software, documentation, Process, etc., to the live environment. Deployment is part of the Release and Deployment Management Process.
Enterprise Service Desk	The Single Point of Contact (SPOC) between Users and Contractors responsible for receiving, logging, escalating, monitoring and closing tickets associated with managing Incidents and Service Requests. Also responsible for communicating with Users regarding the status of Incidents and Service Requests and on-going measurement of Customer satisfaction.
Government	The National Aeronautics and Space Administration (NASA) enterprise along with the collective business units making up the IT Infrastructure and Service delivery environment defined to be in-scope for purposes of the IT Infrastructure Integration Program (I³P) Acquisition.
Incident	An unplanned interruption to an IT Service or a reduction in the quality of an IT Service. Failure of a Configuration Item that has not yet impacted service is also an Incident. For example failure of one disk from a mirror set.
Incident Management	The Process responsible for managing the Lifecycle of all Incidents. The primary objective of Incident Management is to return the IT Service to Users as quickly as possible.

Information Security Management	The Process that ensures the confidentiality, integrity and availability of an organization's assets, information, data and IT Services. Information Security Management usually forms part of an organizational approach to security management which has a wider scope than the IT Service Contractor, and includes handling of paper, building access, phone calls etc., for the entire Organization.
IT Infrastructure	All of the hardware, software, networks, facilities, etc., that are required to develop, test, deliver, monitor, control or support IT Services. The term IT Infrastructure includes all of the information technology but not the associated people, Processes and documentation in support of IT Services.
IT Service	A service provided to one or more Customers by an IT Service Contractor. An IT Service is based on the use of information technology and supports the Customer's business Processes. An IT Service is made up from a combination of people, Processes, and technology and should be defined in a Service Level Agreement.
IT Service Contractor	A Service Provider/Supplier responsible for supplying goods or services that are required to deliver IT Services. These may include commodity hardware and software vendors, network and telecom suppliers and IT outsourcing service providers.
IT Service Continuity Management	The Process responsible for managing risks that could seriously impact IT Services. ITSCM ensures that the IT Service Contractor can always provide minimum agreed Service Levels, by reducing the risk to an acceptable level and planning for the recovery of IT Services. ITSCM should be designed to support business continuity management.
IT Service Management (ITSM)	The implementation and management of quality IT Services that meet the needs of the business. IT Service Management is performed by Contractors in concert with the client enterprise through an appropriate mix of people, Process and information technology.
Knowledge Management	The Process responsible for gathering, analyzing, storing and sharing knowledge and information within an organization. The primary purpose of Knowledge Management is to improve efficiency by reducing the need to rediscover knowledge.
Known Error	A Problem that has a documented root cause and a workaround. Known Errors are created and managed throughout their Lifecycle by Problem Management. Known Errors may be identified by Users, Customers or IT Service Contractors.

Lifecycle	The various stages in the life of an IT Service, Configuration Item, Incident, Problem, Change etc. The Lifecycle defines the categories for status and the status transitions that are permitted. For example: • The Lifecycle of an application includes requirements, design, build, deploy, operate, and optimize. • The expanded Incident Lifecycle includes detect, respond, diagnose, repair, recover, restore. • The lifecycle of a server may include: ordered, received, in test, live, disposed etc.
Operational Level Agreement (OLA)	An agreement between an enterprise IT organization and another part of the same organization. An OLA supports the enterprise IT organization's delivery of IT Services to Customers through IT Service Contractors. The OLA defines the goods and services to be provided and the responsibilities of both parties. Performance expectations are documented in SLAs and other Underpinning Contracts.
Performance Work Statement (PWS)	A document containing all requirements for a product purchase, or a new or changed IT Service.
Problem	A cause of one or more Incidents. The cause is not usually known at the time a problem record is created. The Problem Management Process is responsible for further investigation of the Problem.
Problem Management	The Process responsible for managing the Lifecycle of all Problems. The primary objectives of Problem Management are to prevent Incidents from happening and to minimize the impact of Incidents that cannot be prevented.
Process	A structured set of Activities designed to accomplish a specific objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A Process may define policies, standards, guidelines, Activities, and work instructions if they are needed.
Recovery Point Objective (RPO)	The maximum amount of data that may be lost when an IT Service is restored after an interruption. Recovery Point Objective is expressed as a length of time before the failure.
Recovery Time Objective (RTO)	The maximum time allowed for recovery of an IT Service following an interruption. Recovery Time Objective is expressed as a length of time from the failure to restoration of the IT Service.

Release	A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, tested and deployed as a single entity.
Release and Deployment Management	The Process responsible for both Release Management and Deployment.
Release Management	The Process responsible for planning, scheduling and controlling the movement of releases to test and live environments. The primary objective of Release Management is to ensure that the integrity of the live environment is protected and that the correct components are released. Release Management is part of the Release and Deployment Management Process.
Request For Change (RFC)	A formal proposal for a Change to be made. An RFC includes details of the proposed Change, and may be recorded on paper or electronically.
Request Fulfillment	The Process responsible for managing the Lifecycle of all Service Requests.
Service Asset & Configuration Management	The Process responsible for both Configuration Management and Asset Management.
Service Level	Measured and reported achievement against one or more Service Level Targets.
Service Level Agreement (SLA)	An agreement between a Contractor and a Customer. The Service Level Agreement describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Contractor and Customer. A single SLA may cover multiple IT Services or multiple Customers
Service Level Management	The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews.
Service Level Targets	Service Level Targets are performance commitments documented in a Service Level Agreement. Service Level Targets are based on Service Level Requirements agreed to with the business and ensure IT Service design is aligned with results.

Service Request	A request from a user for information, advice, a standard Change or for access to an IT Service. For example - to reset a password, or to provide standard IT Services for a new user. Service Requests are usually handled by a Service Desk and do not require an RFC (Request For Change) to be submitted.
Single Point of Contact (SPOC)	A designated single, consistent way to communicate with an individual, business entity or enterprise.
Tier 0 (Self Help)	A level of support provided to users via a web-based portal. This Self-Help level of support assists Users resolve lower level of difficulty Incidents and/or Service Requests. The Incidents and/or Service Requests handled at this level of support typically can be resolved through the direct effort of Users, rather than through the effort of resources associated with the Enterprise Service Desk.
Tier 1 Support	The first level in a hierarchy of support groups involved in the resolution of Incidents. Each level contains a more specialized skill, knowledge, time or resource in support of their responsibilities. Tier 1 is typically defined as the Enterprise Service Desk (ESD).
Tier 2 Support	The second level in a hierarchy of support groups involved in the resolution of Incidents and investigation of Problems. Each level contains a more specialized skill, knowledge, time or resource in support of their responsibilities. Tier 2 would be the next level of dispatch/escalation from Tier 1 (ESD) support.
Tier 3 Support	The third level in a hierarchy of support groups involved in the resolution of Incidents and investigation of Problems. Each level contains a more specialized skill, knowledge, time or resource in support of their responsibilities. Tier 3 would be the next level of dispatch/escalation from Tier 2 support.
Underpinning Contract	A Contract between an IT Service Contractor and a third party. The third party provides goods or services that support the delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.
Users	A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly.

9 Referenced Document List

The following documents are referenced within the cross function requirements. These documents may be found in the Technical Library section of the I3P web site at http://i3p.nasa.gov/

a. NASA Enterprise Service Management Concept of Operations
b. NPR 7120.7 NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements
c. NPR 2800.1, Managing Information Technology
d. NPR 2810.1 Security of Information Technology
e. NPR 2830.1 NASA Enterprise Architecture Procedures
f. NPD 1000.0 NASA Strategic Management and Governance Handbook
g. NASA Enterprise Service Desk Concept of Operations
h. NASA Enterprise Service Desk Performance Work Statement
i. NASA Enterprise Architecture Repository (NEAR) Interface Definition Specification
j. Government Availability Management Process
k. Government Capacity Management Process
l. Government Change Management Process
m. Government Incident Management Process
n. Government Information Security Management procedures and policy
o. Government IT Service Continuity Management Process
p. Government Knowledge Management Process
q. Government Problem Management Process
r. Government Release and Deployment Management (RDM) procedures
s. Government Release Plan (part of Government's Release and Deployment Management (RDM) procedures and policy)
t. Government Request Fulfillment Process
u. Government Service Asset and Configuration Management (SACM) Process
v. Government Service Level Management Process
w. Government Supplier Management Process